qTReX : A semi-autonomous continuous-variable quantum key distribution system

Nitin Jain
Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark
nitinj@iitbombay.org

Hou-Man Chin
Department of Photonics, Technical University of Denmark, 2800 Lyngby, Denmark

Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark

Hossein Mani
Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark

Erik Bidstrup
Zybersafe ApS, Erik Husfeldts Vej 7, Denmark

Ulrik L. Andersen
Tobias Gehring
Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark
tobias.gehring@fysik.dtu.dk

Abstract: Continuous-variable quantum cryptography can leverage existing telecommunication technology for solving the cryptographic task of secure key distribution. We present `qTReX`: A low-noise, highly stable, semi-autonomous prototype using optical coherent states for quantum key distribution.

1. Overview

Quantum key distribution (QKD) is a method for solving the cryptographic task of secure key distribution [1, 2]. The QKD users (Alice and Bob) operate a so-called QKD protocol that consists of a quantum communication and a classical communication phase. In the first phase, quantum correlations are established via preparation, transmission, and measurement of quantum states over an insecure quantum channel. Thereafter, Alice and Bob try to extract a common bit sequence—the secret key—from the correlations via classical communication over an authenticated channel. An eavesdropper Eve, assumed to be in complete control of these two channels, attempts to get information of the secret key through attacks. However, Eve's presence can be detected by Alice and Bob through errors in the data processing stage during the classical communication phase. Moreover, if Eve's knowledge surpasses a certain security threshold, then no secret key can be extracted. Otherwise, after erasing Eve's information, Alice and Bob obtain a (smaller but) private key that can be used for symmetric encryption.

The only known quantum system for practically transmitting quantum information over long distances are (optical) photons. In discrete-variable QKD (DVQKD), the information is encoded over a discrete set of modes, e.g., in the photon's polarization or (relative) phase degree of freedom, and the quantum measurements are performed using single photon detectors. In case of continuous-variable QKD (CVQKD) protocols, Alice employs CV properties such as the electromagnetic quadratures of the optical field for encoding the key bits, while Bob does some form of coherent detection such as homodyning or heterodyning for decoding [3]. Currently, provable security against the most general attacks of Eve can be obtained only for a Gaussian-shaped constellation of coherent states [4]. Such Gaussian-modulated coherent states (GMCSs) have been at the forefront of numerous CVQKD implementations [5–10].

In this demo, we present `qTReX`: a state-of-the-art GMCS-CVQKD system with Alice's transmitter and Bob's receiver housed in two standard 19" boxes of 3U installed in a telecom rack. Two workstations containing PCI Express based digital-to-analog converter (DAC) and analog-to-digital converter (ADC) cards are used for state preparation and state measurement, respectively. The classical data processing steps are shared by Alice and Bob in accordance to the information reconciliation strategy [5, 11]. The generated keys are fed to hardware encryption

devices [12] that can then secure a confidential datastream using 256-bit advanced encryption standard (AES) keys, refreshed every 2 minutes or no later than after 2^{32} transmitted frames.

Figure 1 shows a few details of our CVQKD-enabled secure key distribution solution. The transmitter and

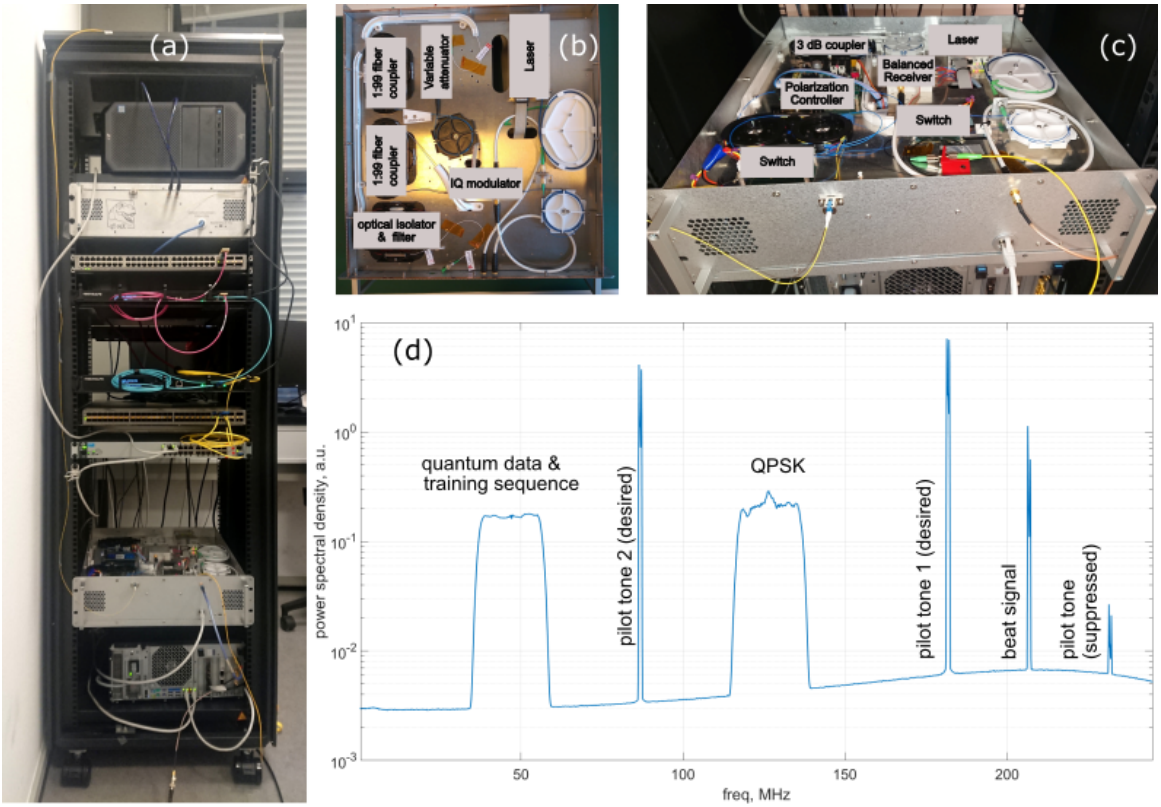

Fig. 1. (a) Standard 19" telecom rack containing the `qTReX` CVQKD system, together with the workstations housing the RF data modulation and acquisition cards and network encryption devices. (b) `qTReX` transmitter and (c) `qTReX` receiver optical setups. (d) RF heterodyne spectra of the modulated signal; important spectral components have been labelled. More details about the system and operation are available in Refs. [9, 10]

receiver boxes comprise a solid plate with the optical/optoelectronic components on one side (as shown in Fig. 1(b) and Fig. 1(c), respectively) and the necessary control electronics on the other. A system on a chip acts as the central computer for controlling and monitoring the hardware. We use Qudi [13], a Python3 based modular, multi-operating system software suite for experimental control and basic data processing. Figure 1(d) shows a power spectral density estimate obtained from the ADC data samples, captured and processed using the Qudi framework.

2. Demo content & implementation

During the quantum phase of the QKD protocol, the steps of RF data modulation and acquisition are performed autonomously. To ensure correct as well as optimal operation, the CVQKD system also frequently calibrates the shot noise and electronic noise. The digital signal processing (including the steps of carrier phase recovery, clock recovery, temporal synchronization, down-conversion and downsampling), classical data processing (including parameter estimation, information reconciliation, and privacy amplification), and uploading the secret key to the hardware encryption devices are currently performed offline.

Our primary objective would be to demonstrate the steps of quantum state preparation, detection, and calibration via live data visualizations to the attendees. The physical setup would be a subset of the telecom rack of Fig. 1(a), laid horizontally on a table, with computer screens connected to the two workstations. The demo itself will consist of the following steps: tuning the local oscillator (LO) wavelength so that the beat note between the signal and LO lasers is inside some pre-defined frequency range, optimization of signal polarization by maximising the power of the beat note, modulation and acquisition of data frames by the transmitter and receiver, respectively, and capturing shot noise and electronic noise traces for calibration.

For these tasks, we shall utilize the Qudi framework that comes with an easy-to-use graphical user interface. In addition, we shall also showcase the online monitoring of various system parameters such as temperature, power

supply voltages, detector photocurrents. For this, we shall use open source software such as influxDB and Grafana that allow capturing and interactive visualization of time series data through charts, graphs, etc.

3. Innovation & relevance to OFC

From the perspective of a QKD system, `qTReX` combines several innovations (both in software and hardware) that provide a semi-autonomous and robust operation featuring stability and low excess noise. They are:

- Frequency-multiplexed pilot tones and a quadrature phase shift keying (QPSK) alphabet for carrier phase recovery and clock recovery [9, 14].
- Time-multiplexed training sequence for temporal synchronization.
- High-extinction optical switches on the signal and (true) LO for frequent and independent shot noise calibration.
- Power monitor, wavelength filter, and isolator for prevention of Trojan-horse attacks [15].

CVQKD can be understood as a form of coherent optical communication, i.e., using the amplitude and phase of light to transmit information. The main difference is that instead of preparing and measuring classical light fields, CVQKD systems operate in the quantum regime, i.e., perform quantum-noise-limited measurements of non-orthogonal quantum states. Therefore, as the channel loss increases, the ability of CVQKD systems to transmit useful information (measured in terms of the achievable secret key rate) decreases sharply. Nonetheless, at access network scales (<50 km long quantum channels), CVQKD systems are the most cost-effective solution for widespread deployment of quantum cryptography. Furthermore, the similarity of CVQKD to coherent telecommunication, for instance, usage of broadband IQ modulators, room temperature operation (especially in contrast to DVQKD systems), increases the feasibility of network integration in the future.

OFC has traditionally been a classical optical communication conference. In the recent years though, there has been an increased focus on quantum communication, especially due to the developments in quantum cryptography. Our prototype `qTReX`, parked right at this quantum-classical boundary, not only draws and unifies the best from these two worlds but also leads to new developments, e.g. the carrier phase recovery and clock recovery techniques using machine learning [9, 14]. We therefore believe that our demo shall be of great relevance to OFC.

References

1. V. Scarani *et al.*, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).
2. S. Pirandola *et al.*, "Advances in quantum cryptography," Adv. Opt. Photonics **12**, 1012 (2020).
3. T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**, 010303 (1999).
4. A. Leverrier, "Security of continuous-variable quantum key distribution via a gaussian de finetti reduction," Phys. Rev. Lett. **118**, 200501 (2017).
5. F. Grosshans *et al.*, "Quantum key distribution using gaussian-modulated coherent states," Nature **421**, 238–241 (2003).
6. A. M. Lance *et al.*, "No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light," Phys. Rev. Lett. **95**, 180503 (2005).
7. P. Jouguet *et al.*, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Photonics **7**, 378–381 (2013).
8. D. Huang *et al.*, "High-speed continuous-variable quantum key distribution without sending a local oscillator." Opt. letters **40**, 3695–8 (2015).
9. H.-M. Chin *et al.*, "Machine learning aided carrier recovery in continuous-variable quantum key distribution," npj Quantum Inf. **7**, 20 (2021).
10. N. Jain *et al.*, "Practical continuous-variable quantum key distribution with composable security," arXiv:2110.09262 (2021).
11. P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a gaussian modulation," Phys. Rev. A **84**, 062317 (2011).
12. "Datasheet Zybersafe TrafficCloak – Ethernet Encryption," https://zybersafe.com/wordpress/wp-content/uploads/2019/11/Zybersafe-Data-Sheet.pdf. Accessed: 2021-11-15.
13. J. M. Binder *et al.*, "Qudi: A modular python suite for experiment control and data processing," SoftwareX **6**, 85–90 (2017).
14. H.-M. Chin *et al.*, "Clock Recovery for Gaussian Modulated CV-QKD systems," Submitted to OFC 2022 pp. 1–3.
15. N. Jain *et al.*, "Risk analysis of Trojan - horse attacks on practical quantum key distribution systems," IEEE J. on Sel. Top. Quatum Electron. **21**, 1077–260X (2014).