Challenges in Coding, DSP and Parallel Operation of Quantum Key Distribution and Coherent Data Transmission

Tobias A. Eriksson[1], Ruben S. Luís[2], Georg Rademacher[2], Benjamin J. Puttnam[2], Kadir Gumüş[3], Laurent Schmalen[3], Alex Alvarado[4], Hideaki Furukawa[2], Naoya Wada[2], Takuya Hirano[5], Masahide Sasaki[2], Masahiro Takeoka[2].

(1) Infinera Corp., Fredsborgsgatan 24, 117 43 Stockholm, Sweden. teriksson@infinera.com
(2) National Institute of Information and Communications Technology (NICT), 4-2-1 Nukui-kitamachi, Koganei, Tokyo 184-8795, Japan.
(3) Karlsruhe Institute of Technology (KIT), Communications Engineering Lab (CEL), Hertzstr. 16, 76187 Karlsruhe, Germany.
(4) Eindhoven University of Technology, 5600 MB Eindhoven, The Netherlands.
(5) Gakushuin University, Department of Physics, 1-5-1 Mejiro,Toshima-ku, Tokyo, 171-8588, Japan.

Abstract *We discuss challenges and recent progress on coding, digital signal processing and joint transmission with classical data channels, for quantum key distribution.*

Introduction

The security of today's and future communication systems is threatened by rapid technological advances, including disruptive technologies such as quantum computation[1]. This threat is especially emergent for applications concerning information that is classified as sensitive, such as in military, governmental, insurance, banking or medical use cases[2]. This threat has accelerated research and development of encryption systems that employ quantum key distribution (QKD) technology[2–6]. Although current encryption technologies *probably* can be deemed secure with the currently available computational power, it is already threatened by the so-called *"store now, decrypt later"* attack where an adversary stores encrypted data and simply waits until sufficient technological advances have been made to break the encryption. Further, if a sudden disruption is made in quantum computing, it would leave the current communication infrastructure vulnerable.

Most experimental work on QKD is performed on dedicated point-to-point links. However, we can also distribute keys using a trusted person, sometimes called a trusted courier, that distributes the keys between two locations[7]. Whilst this may appear inefficient, lets consider that this person loads purely random bit sequences on a hard drive with 10 TB space and drives with an average speed of 80 km/h over a distance of 80 kilometers, assuming it takes 30 minutes time sign out the hard drive and get to and from the car, we actually get a secret key rate of 14.8 Gbit/s which is much higher than state of the art QKD systems typically operating in the Mbit/s region. Although this example might seem a bit artificial, besides QKD, using a trusted courier to deliver keys is the only known unconditionally secure method of distributing keys and is actually used in high security applications. The situation is of course different if we look at key distribution in a network with many nodes where it soon becomes impractical to courier keys between all nodes and in this scenario, QKD becomes an attractive option. It is then crucial that the QKD system can leverage the existing network infrastructure, otherwise a completely new network needs to be constructed for key distribution which would significantly increase costs and also prohibits dynamic adaptation of QKD technologies. This motivates investigation of joint transmission of quantum and classical signals, since many networks may not have spare fiber that can be used for the QKD channels.

Co-propagation of QKD and Classical Channels

QKD systems are typically categorized into discrete variable (DV) and continuous variable (CV), where DV systems use single photons and CV systems coherent states. The most straightforward method of co-propagation of QKD and classical channels is to use wavelength division multiplexing (WDM). Links where classical channels are using the C-band and a DV-QKD channel is transmitted at 1300 nm, have been demonstrated with 20 and 32 coherent classical channels[8,9]. Further, co-propagation within the C-band has also been demonstrated for DV-QKD with a mix of 100 Gbit/s channels and unmodulated laser tones to emulate classical channels[10].

One disadvantage of DV-QKD in co-propagation is that the single-photon detectors are broadband and narrow-band filtering is required at the receiver side[8]. Nevertheless, co-propagation with a single channel with limited power has been demonstrated using off-the-shelf filters[11] and a field-trial with four 10 Gbit/s on-off keying channels have been demonstrated[12]. Further, DV-QKD has been demonstrated over deployed fiber with classical data in the same fiber[8,13].

One strength of CV-QKD, compared to DV-QKD, is the ability of spectral filtering using a local oscillator, which is convenient for co-propagation with classical signals. Joint propagation together with intensity modulated classical signals has been demonstrated in different channel configurations[14,16] such as with 7 $\times$ 12.5 Gbit/s on-off keying signals in the C-band[15]. Co-propagation with up to 56 classical 100 Gbit/s coherent channels in the C-band and the CV-QKD channel in the S-band to avoid ASE noise from the C-band EDFAs has been shown[17]. We have demonstrated co-propagation in the C-band of one CV-QKD and up to 100 classic PM-16QAM channels amounting to 18.3 Tbit/s classical data rate[18,19].

We have previously discussed different challenges in parallel operation of QKD and classical data channels[20]. See also[21,22] for summaries of recent progress on this topic. It is important to note that there exists no clear optimal solution for co-propagation, and in cases where there already exists an operating link, there might not be room for flexibility when it comes to the classical channels. For QKD, its optimal to operate in the C-band due to the low fiber loss as the fundamental limitation on the secret key rate (SKR) is governed by the loss. Unfortunately, most classical systems are also using the C-band, except intensity modulated schemes that use the O-band due to the lower dispersion. One main challenge in operating both classical and quantum channels in the C-band is the presence of ASE noise from the EDFAs which requires notch filters for the QKD channel[10,18,19]. A limiting distortion from the classical channel is Raman scattering[23] which peaks at around 20 km for conventional SMF[16]. To combat Raman scattering, the wavelength allocation of the classical and quantum channels can be managed, as well as limiting the total number of channels and the total optical power. Further, nonlinear cross-talk from four-wave mixing[24] and Brillouin scattering[25] can influence the quantum channel.

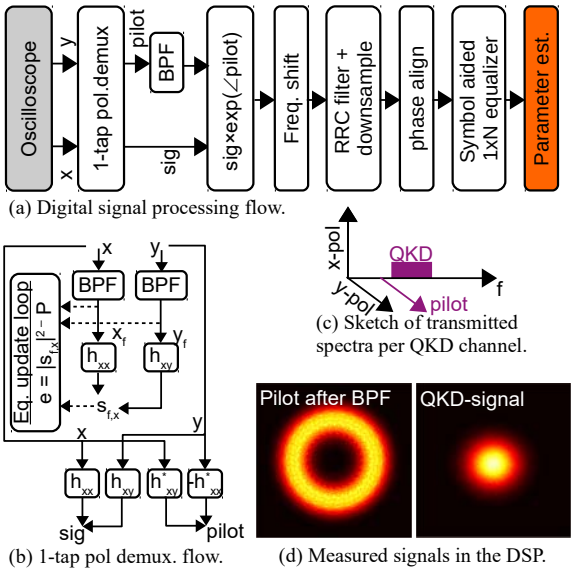

Fig. 1: Outline of DSP showing (a) the DPS chain, (b) outline of the 1-tap polarization demultiplexing stage (c) a sketch of the spectra and (d) an example constellation from measured data. Figure from[30]

DSP challenges for CV-QKD

One of the biggest challenges for CV-QKD is how to establish a phase reference between two remote parties. The phase references can be addressed using either optical[26,27] or digital[17,28] techniques. For polarization drifts however, optical solutions are typically applied using either manual alignment at the receiver side or all-optical solutions based on feedback[27]. The latter works fine for a single channel but scales badly if several QKD channels are desired. We have proposed a full digital CV-QKD system based on dual-polarization, dual-quadrature detection using a polarization multiplexed pilot tone[29]. The pilot tone is used both to find the taps of a 1-tap butter-fly FIR filter used for polarization-multiplexing and to do frequency offset compensation and phase tracking, as outlined in Fig. 1. This type of receiver has enabled us to demonstrate WDM of 194 separate CV-QKD channels without manual or optical tuning[30].

Coding challenges for CV-QKD

One of the biggest challenges for real-time CV-QKD operation is the error correction which, compared to error correction in classical systems, uses extremely large block lengths and an immense number of decoding iterations which are needed due to the extremely low SNR[31,32]. Although QKD systems traditionally run at lower speeds compared to classical systems, the pulse rate of QKD systems is continuously pushed to higher numbers. For real-time CV-QKD to see

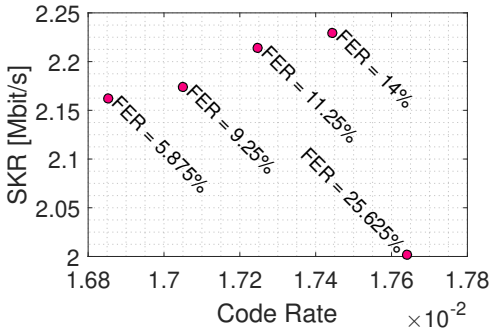

Fig. 2: Trade-off between reconciliation efficiency and FER and its impact on the SKR. Results from the experiments in[29].

any widespread use, practical coding schemes have to be found. Many different coding schemes have been considered such as low-density parity-check (LDPC) codes[32,33,36], polar codes[34], and raptor codes[35]. It is important to note that compared to error correction in classical communication, QKD systems are not sending messages but rather sharing randomness. This means that it is fine to throw away data that did not decode successfully. The SKR with error correction is given as

$$\mathrm{SKR} = (1 - \mathrm{FER})(\beta I_{AB} - \chi_{BE}), \qquad (1)$$

where FER is the frame error rate of the coding scheme, β the reconciliation efficiency (which is a measure of how close to the mutual information the code is operating), I_{AB} the mutual information between Alice and Bob (the legitimate party trying to share keys) and χ_{BE} the Holevo information between the Eavesdropper and Bob (assuming reverse reconciliation)[33]. Ideally, of course we would like to find codes with low FER and high reconciliation efficiency while in reality it is a trade-off between β and FER. This can be seen in Fig. 2 which is taken from our experiments in[29]. Here the code rate of the of a rate 0.02 LDPC code[33] is tuned finely using shortening. As seen, the highest SKR is achieved with an FER of around 14% for this specific link.

Future directions

This discussion on future directions will mainly target CV-QKD, although some of the points are valid also for DV-QKD.

1. **Fully digital QKD systems:** This enables plug-and-play, dynamic adaptation of new QKD channels, and it is easier to integrate with existing network architecture. It is a key technology to lower the cost of QKD systems and to enable large scale wavelength multiplexing of QKD channels.
2. **Low complexity error correction:** The error correction needs to be of a complexity that can be implemented with reasonable power consumption and chip area. Current research results mainly reuse solutions from classical communication and adapt them to the extremely low SNR of QKD. Here, there is most likely a lot of room for improvement with coding schemes tailored for the QKD channel. For instance, we can use the fact that we are sharing randomness and not transmitting messages, which manifests in the previous discussion that it is OK to discard data or frames. Further, an alternative to fine granularity rate adaption is to artificially add noise to match the rate of the code which will lower the information between the eavesdropper and the legitimate parties effectively increasing the SKR[37]. Another example is using post-selection of received samples[38] to increase the SNR, although this comes with security proof caveats.
3. **Security proofs in practice:** There is a large discrepancy between theoretical security proofs of different protocols and actual implementations of said protocols. In practice, imperfect devices are used which has many implications. One example is that it is not possible to achieve a continuous Gaussian modulation due to the limited resolution of DACs. Further, the protocols are bound to use finite lengths for the processing compared to infinite length used in many proofs. Fortunately, there is a lot of activity on this topic currently[39–41].
4. **Integration into existing network architecture:** We have discussed in detail co-propagation of quantum and classical channels which is a key problem to solve for wide-spread adaptation of QKD. However, there are many other open questions such as how to manage the network traffic control in presence of QKD channels and arrange the key management.
5. **Solving the limited distance:** QKD systems are inherently limited by loss which limits the reach. There is no clear way forward to overcome this issue and many different solutions such as using trusted nodes[42,43], quantum repeaters[44], employing novel new protocols such as twin-field QKD[45], and utilizing satellites for QKD[46,47].

Conclusions

We have discussed co-existence of QKD and classical channels and discussed current DSP and coding challenges for QKD systems. Further, we have outlined important topics for future QKD systems.

References

[1] C. Cesare, “Encryption faces quantum foe,” Nature, vol. 525, no. 7568, p. 167 (2015).

[2] E. Diamanti, et al., “Practical challenges in quantum key distribution,” npj Quantum Information vol. 2, p. 16025 (2016).

[3] S. Pirandola, et al., “Advances in quantum cryptography,” arXiv:1906.01645 (2019).

[4] N. Gisin, et al., “Quantum cryptography,” Reviews of Modern Physics vol. 74, no. 1, p. 145 (2002).

[5] H-W. Lo, et al., “Secure quantum key distribution,” Nature Photonics, vol. 8, no. 8, pp. 595-604 (2014).

[6] Q. Zhang, et al., “Large scale quantum key distribution: Challenges and solutions,” Optics Express, vol. 26, no. 18, pp.24260–24273, (2018).

[7] R. Alléaume, et al. “Using quantum key distribution for cryptographic purposes: A survey,” Theoretical Computer Science, vol. 560, pp. 62–81, (2014).

[8] Y. Mao, et al.,‘Integrating quantum key distribution with classical communications in backbone fiber network,” Optics Express, vol. 26, pp. 6010–6020 (2018).

[9] L.-J. Wang, et al, “Long-distance copropagation of quantum key distribution and terabit classical optical data channels,” Physical Review A, vol. 95, 012301 (2017)

[10] J. F. Dynes, et al., “Ultra-high bandwidth quantum secured data transmission,” Scientific Reports, vol 6, 35149 (2016).

[11] B. Fröhlich, Bernd, et al., “Long-distance quantum key distribution secure against coherent attacks,” Optica vol. 4, no. 1, pp. 163–167 (2017).

[12] I. Choi, et al. “Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber,” Optics Express vol. 22, no. 19, pp. 23121–23128, (2014).

[13] J. F. Dynes, et al. “Cambridge quantum network,” npj Quantum Information, vol. 5, no. 101, (2019).

[14] D. Huang, et al., “Field demonstration of a continuous-variable quantum key distribution network,” Optics Letters, vol. 41, pp. 3511–3514 (2016).

[15] T. A. Eriksson, et al., “Coexistence of continuous variable quantum key distribution and 7 $\times$ 12.5 Gbit/s classical channels,” proc. IEEE Summer Topical Meeting Series (SUM) (2018).

[16] F. Karinou, et al., “Toward the integration of CV quantum key distribution in deployed optical networks,” IEEE Photonic Technology Letters, vol. 30, pp. 650–653 (2018).

[17] S. Kleis, et al., “Experimental investigation of heterodyne quantum key distribution in the S-Band embedded in a commercial DWDM system,” proc. Optical Fiber Communication Conference (OFC) (2019), paper Th1J.3.

[18] T. A. Eriksson, et al., “Joint propagation of continuous variable quantum key distribution and 18 $\times$ 24.5 Gbaud PM-16QAM channels,” proc. European Conference on Optical Communication (ECOC) (2018), paper We2.37.

[19] T. A. Eriksson, et al., “Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels,” Communications Physics, vol. 2, no. 1, 9 (2019).

[20] T. A. Eriksson, et al., “Challenges in Parallel Operation of Quantum Key Distribution and Data Transmission,” Proc. of Signal Processing in Photonic Communications, (2019), paper QtW3E-2.

[21] R. Alléaume, et al. “Technology trends for mixed QKD/WDM transmission up to 80 km,” Proc. Optical Fiber Communications Conference and Exhibition (OFC), (2020), paper M4A.1.

[22] A. Bahrami, et al. “”Quantum key distribution integration with optical dense wavelength division multiplexing: a review,” IET Quantum Communication (2020).

[23] B. Qi, et al., “Feasibility of quantum key distribution through a dense wavelength division multiplexing network,” New Journal of Physics vol. 12, 103042 (2010).

[24] Y. Li, et al., “Influence of guided acoustic wave Brillouin scattering on excess noise in fiber-based continuous variable quantum key distribution,” Journal of the Optical Society of America B (JOSA B), vol. 31, no. 10, pp. 2379–2383 (2014).

[25] R. Kumar, et al., “Coexistence of continuous variable QKD with intense DWDM classical channels,” New Journal of Physics vol. 17 no. 4, p. 043027, (2015).

[26] D. Huang, et al., “Continuous-variable quantum key distribution with 1M bps secure keyrate,” Optics Express, vol.23 . no. 13, pp.17511-17519, (2015).

[27] T. Hirano, et. al., “Implementation of continuous-variable quantum key distribution with discrete modulation,” Quantum Science and Technology, vol. 2, no. 2, p. 024010, (2018).

[28] Q. Zhen, et al., “RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection,” Optics Letters, vol.41, np. 23, pp. 5507–5510, (2016).

[29] T. A. Eriksson, et al., “Digital Self-Coherent Continuous Variable Quantum Key Distribution System,” Proc. of Optical Fiber Communication Conference (OFC), (2020), paper T3D. 5.

[30] T.A. Eriksson, et al., “Wavelength Division Multiplexing of 194 Continuous Variable Quantum Key Distribution Channels,” Journal of Lightwave Technology, vol. 38, no. 8, pp. 2214–2218, (2020).

[31] A. Leverrier and P. Grangier, “Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation,” Phys. review letters 102, p. 180504 (2009)

[32] M. Milicevic, et al. “Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography,” npj Quantum Inf vol. 4, no. 21, (2018).

[33] P. Jouguet, “Long distance continuous-variable quantum key distribution with a Gaussian modulation,” Phys. Rev. A, vol. 84, (2011).

[34] P. Jouguet, “High performance error correction for quantum key distribution using polar codes,” Quantum Inf. Comput, vol. 14, (2012).

[35] C. Zhou, et al., “Continuous-variable quantum key distribution with rateless reconciliation protocol,” Phys. Rev. Appl., vol. 12, (2019).

[36] X. Jiang, et al., “High speed reconciliation for CVQKD based on spatially coupled LDPC codes,” IEEE Photon. J., vol. 10, pp. 7600410, (2018).

[37] S. Kreinberg, et al., “Adding artificial noise for dynamic code rate matching in continuous-variable quantum key distribution,” CLEO: Applications and Technology, (2020), paper ATh1I-6.

[38] N. Walk, et al., “Security of continuous-variable quantum cryptography with Gaussian postselection,” Physical Review A, vol. 87, no. 2, pp.020303, (2013).

[39] V. Scarani and R. Renner, “Security Bounds for Quantum Cryptography with Finite Resources,” arXiv preprint arXiv:0806.0120, (2008).

[40] T. Matsuura, et al., “Finite-size security of continuous-variable quantum key distribution with digital signal processing,” arXiv preprint arXiv:2006.04661, (2020).

[41] C. C-W. Lim., “Security analysis of quantum key distribution with small block length and its application to quantum space communications,” arXiv preprint arXiv:2009.04882, (2020).

[42] J. Qiu., “Quantum communications leap out of the lab,” Nature, vol. 508, no. 7497, pp. 441–442, (2014).

[43] M. Sasaki, et al., “Field test of quantum key distribution in the Tokyo QKD network,” Opt. Express, vol. 19, pp. 10387–10409 (2011).

[44] H. J. Briegel, et al., “Quantum repeaters: the role of imperfect local operations in quantum communication,” Phys. Rev. Lett. vol. 81, pp. 5932–5935, (1998).

[45] M. Lucamarini, et al, “Overcoming the rate-distance limit of quantum key distribution without quantum repeaters,” Nature vol.557, no. 7705, pp. 400–403, (2018).

[46] J. Yin, et al., “Satellite-based entanglement distribution over 1200 kilometers,” Science, vol.356, pp. 1140-1144, (2017).

[47] S-K. Liao, et al., “Satellite-to-ground quantum key distribution,” Nature vol.549, no. 7670, pp. 43–47, (2017).