Modelling Weak-Coherent QKD Systems Using a Classical Simulation Framework

Igor Koltchanov[a], Piotr Novik[b], Chris Maloney*[c], André Richter[a]
[a]VPIphotonics GmbH, Germany, [b]VPI Development Center, Belarus, [c]VPIphotonics Inc., USA
*e-mail: chris.maloney@vpiphotonics.com

Motivation

Quantum key distribution (QKD) systems are commercially available and have been implemented with several different protocol classes. One important class is weak coherent-based QKD protocols as these schemes enable the usage of conventional lasers thus, eliminating the need for quantum light sources. Conveniently, weak-coherent prepare and measure protocols enable the use of classical optical simulation tools in order to engineer QKD systems.

In collaboration with the EU Quantum Flagship Project UNIQORN, VPIphotonics has developed *VPItoolkit QKD* to enable system-level CV-QKD and DV-QKD simulations as an add-on to the *VPItransmissionMaker Optical Systems* simulation environment. It provides models for QKD transmitters/receivers, parameter and secret key rate estimation, and application examples. The simulation of weak-coherent QKD using our classical simulation framework supports the design of QKD optical systems, while considering the imperfections of components. It allows the optimization of system parameters, like signal intensity or basis probability while enabling the development and validation of algorithms for phase recovery, PMD mitigation, and so on.

Applications

- ✓ System design: various implementation options for QKD systems and sub-systems
- ✓ Study co-existence scenarios: Raman scattering and cross-talk from classical channels
- ✓ Account of component imperfections: thermal and quantization noise, RIN, phase noise, biased beam splitting ratios, dark count rates, after pulsing…
- ✓ Optimization of the system parameters: modulation amplitude, photons per pulse, filter bandwidth, BB84 basis probability, symbol rate, etc.
- ✓ Estimation of max possible secret key rate, transmission distance, etc.

Classical Simulation Framework for Weak-Coherent QKD

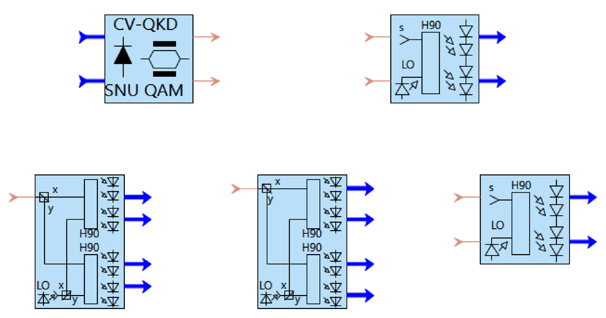
- Practical QKD technology
- Coherent states $|\alpha\rangle = |q + ip\rangle$ are "labeled" by quadratures q, p that can be represented by Re/Im components of the "classical" amplitude $A = q + ip \Rightarrow$ *no changes in the signal model required*
- For linear components, transformation rules $|\alpha_{in}\rangle \rightarrow |\alpha_{out}\rangle$ are the same as for classical signals $A_{in} \rightarrow A_{out}$ $\Rightarrow$ *no changes in the model algorithms*
- Time-series of coherent states with multiple states per symbol $\Rightarrow$ *realistic waveforms, filtering, jitter,…*
- Quantum fluctuations are modeled in the receivers by shot noise (CV-QKD) or by photon counting (DV-QKD)
- Electrical excess noise (thermal,…) is modeled as voltage fluctuations
- Optical excess noise (Raman, RIN…) is modeled as quadrature fluctuations
- *VPItoolkit QKD:* QKD-specific modules

References

1. Hugues-Salas E. et al., *Co-existence of 9.6 Tb/s Classical Channels…* (2018)
2. Lucamarini M. et al., *Efficient decoy-state QKD…* (2013)
3. Laudenbach F. et al., *CV-QKD with Gaussian Modulation* (2018)
4. Roberts G.L et al., *Direct GHz-clocked phase…* (2018)
5. Inoue K., *DPS QKD Systems* (2015)

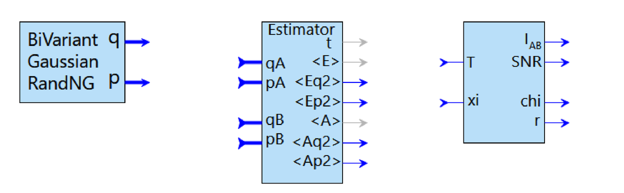
CV-QKD Building Blocks

CV-QKD Rx & Tx



- Idealized coherent/heterodyne Rx & Tx
- Self-calibrating realistic polarization-diverse coherent/heterodyne receiver
  - Based on pol-diverse Rx
  - Based on realistic coherent/heterodyne Rx

CV-QKD Symbol selection and post processing



- Random number generator for sampling Gaussian-modulated quadratures
- Estimation of channel transmittance and excess noise
- Secret key rate calculation: asymptotic or finite size

250 MBd CV-QKD in coexistence with 8x200 Gbit/s PM-16QAM

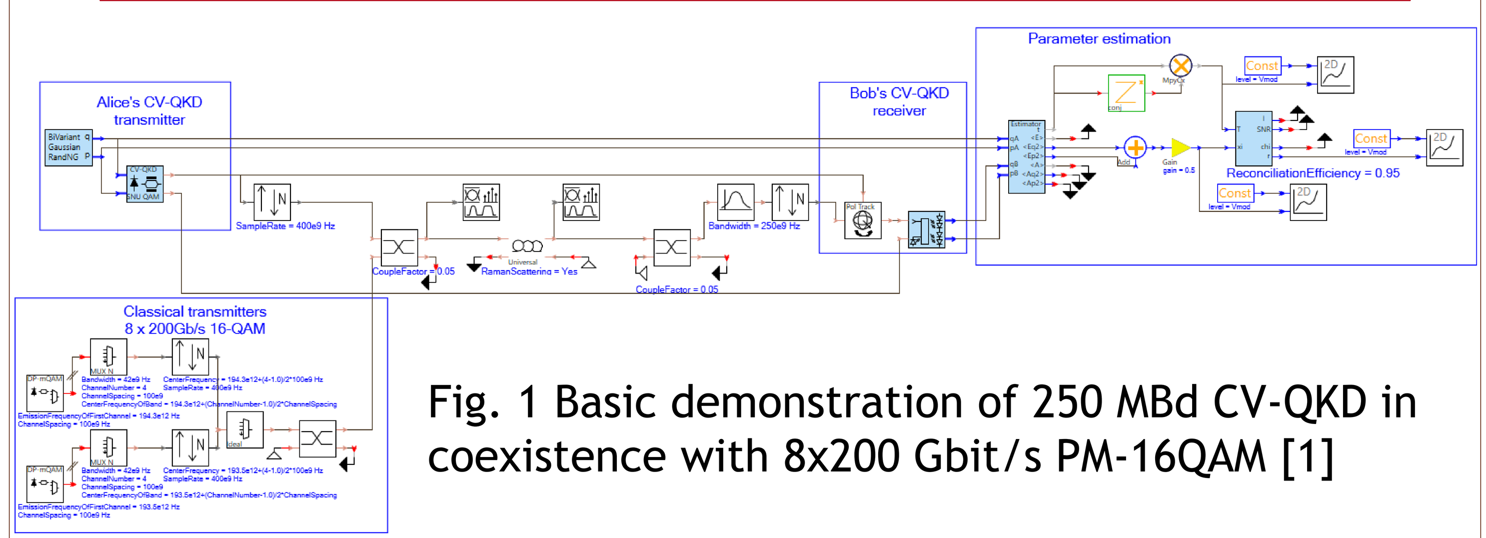


Fig. 1 Basic demonstration of 250 MBd CV-QKD in coexistence with 8x200 Gbit/s PM-16QAM [1]

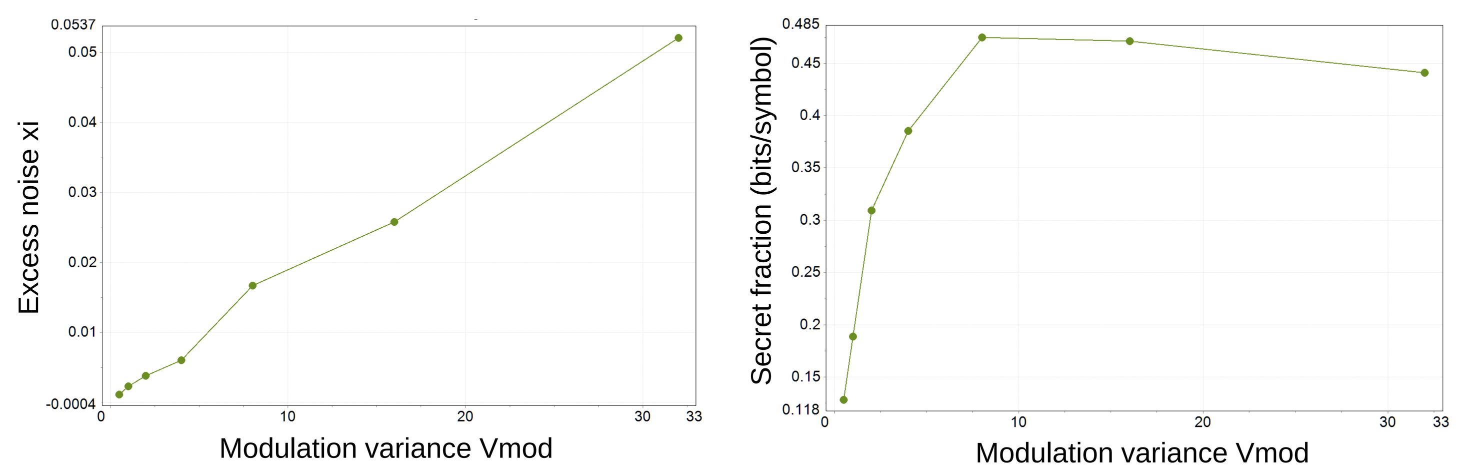


Fig. 2 Modulation variance sweep highlighting the relationship with both excess noise (left) and secret fraction (right).

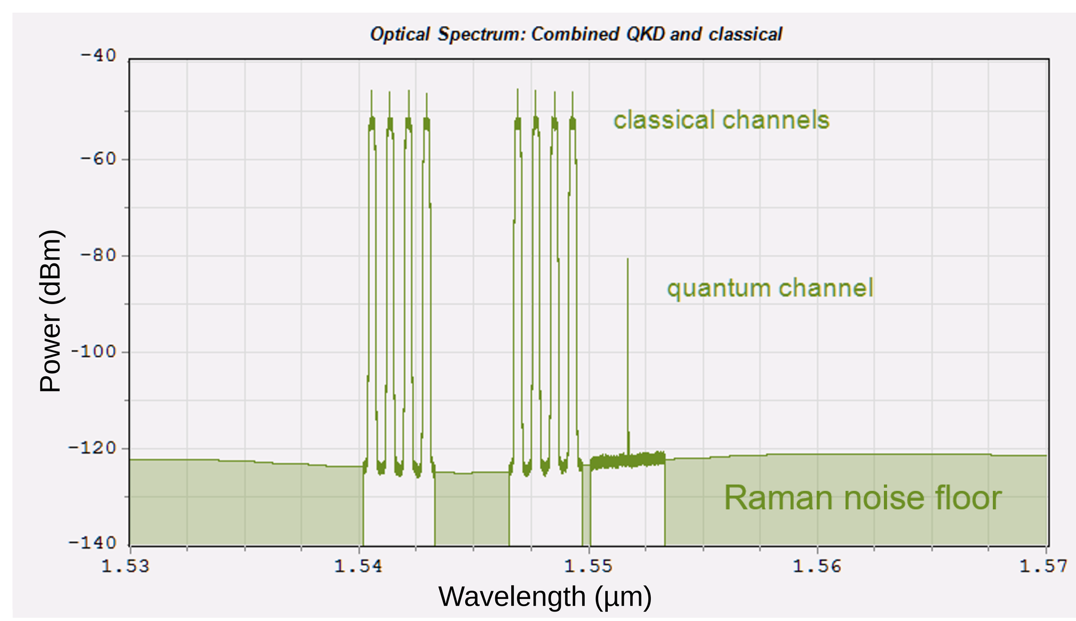
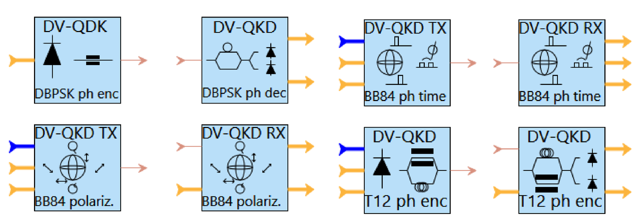


Fig. 3 Optical Spectrum of the combined quantum and classical channels after transmitting through fiber.

The degradation of the quantum channel due to Raman scattering from the classical channels is accounted for. The Raman noise is calculated using a classical fiber model.
The key rate estimation assumes a block length of 100 million symbols and reconciliation efficiency of 95%.

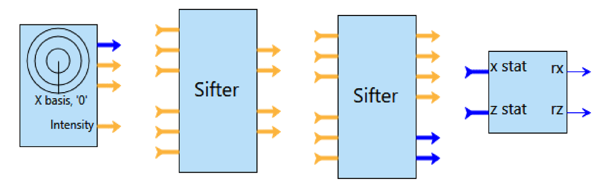
DV-QKD Building Blocks

DV-QKD Rx & Tx



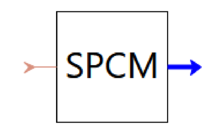
- Differential phase shift (DPS)
- BB84-like with decoy
- Polarization encoding
  - Phase/time encoding
  - T12

DV-QKD Symbol selection and post processing



- Random number generator for (T12-like) BB84 protocols
- Secret fraction estimator for T12 DV-QKD
- Sifters

DV-QKD detector: SPAD

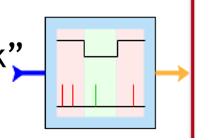


Input: Optical signal
Output: Time stamps

SPAD model includes:
- Dead time
- Gaussian timing jitter
- Exponential timing jitter
- After-pulsing
- Dark counts

Analysing time stamps

Input: Time stamps
Output: "click" / "no click" for each symbol time bin



Acceptance window can be reduced for better dark count suppression.

T12 BB84-like DV-QKD

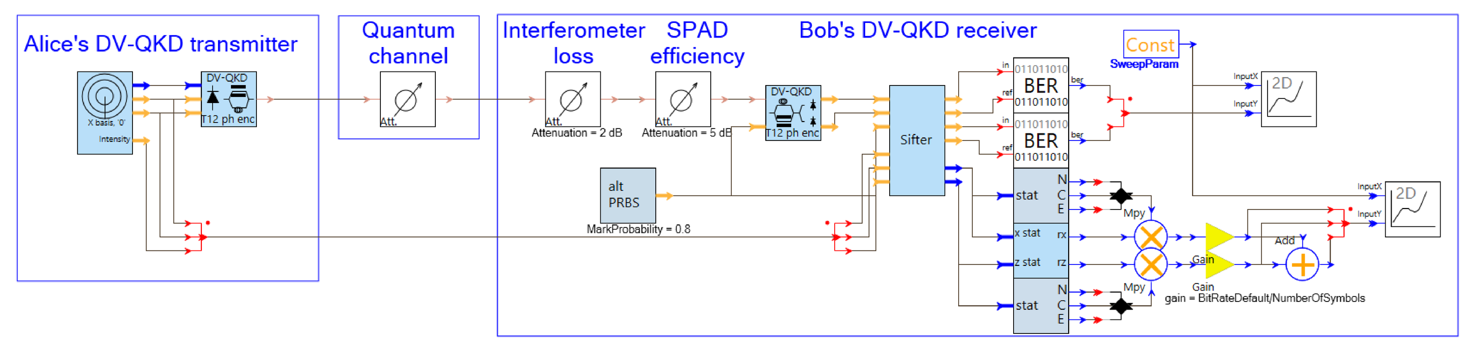


Fig. 4 Basic demonstration of T12 BB84-like DV-QKD which relies on weak coherent states in the prepare-and-measure scheme [2]

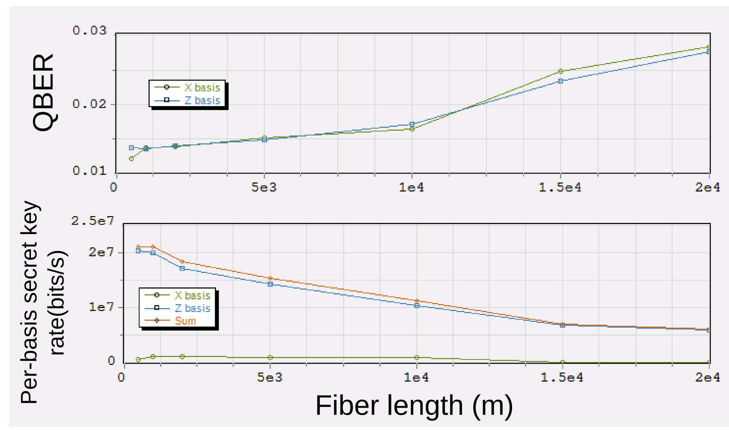


Fig. 5 Fiber length sweep showing how transmittance affects QBER. The larger the losses, the higher the fraction of detection events originating from dark counts or optical noise sources.

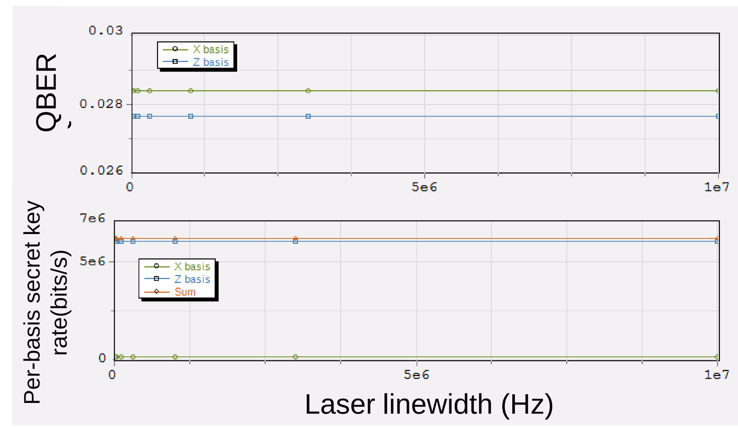


Fig. 6 Laser linewidth sweep showing how phase diffusion affects QBER. Since T12 is basically polarization encoding, weak phase correlation between subsequent symbols does not affect QBER.

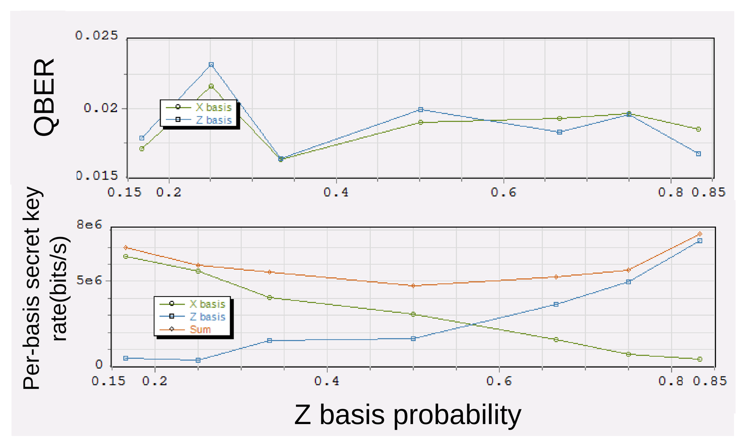


Fig. 7 Z basis probability sweep illustrating how bias towards one basis impacts the secret key rate.

We investigate the effect of fiber length, laser linewidth and Z basis probability for this T-12 BB84-like DV-QKD system. It should be noted that a basis imbalance results in an increase in the secret key rate.

Acknowledgement: Funding from European Union's Quantum-Flagship project UNIQORN under grant agreement No 820474.