Low-noise, low-complexity CV-QKD architecture

Hans H. Brunner, Lucian C. Comandar, Fotini Karinou, Stefano Bettelli, David Hillerkuss, Fred Fung,
Dawei Wang, Spiros Mikroulis, Maxim Kuschnerov, Andreas Poppe, Changsong Xie, Momtchil Peev
Huawei Technologies Duesseldorf GmbH, Munich, Germany
Email: hans.brunner@huawei.com

***Abstract*—In contrast to *discrete-variable quantum key distribution* (DV-QKD), which requires specialized hardware like single-photon detectors, the *continuous-variable* version (CV-QKD) promises low-cost and high-performance implementations by leveraging mature telecommunication technology.**

Here, a simplified CV-QKD architecture based on analog frontends and digitizers for mobile communication systems and standard optical components is proposed. The high-fidelity, software-defined receiver and transmitter allow to shift complexity from the analog to the digital domain. This not only improves the robustness and paves the way for a low-cost implementation. The simplification of the optics also reduces the probability of side channel attacks in the optical domain. The noise and loss of every step shifted to the digital domain can be reduced arbitrarily close to its minimum, which emphasizes the role of the *digital-to-analog* (DAC) and *analog-to-digital conversion* (ADC).

I. Introduction

In CV-QKD protocols like GG02 [1] and the non-Gaussian form [2] information is encoded in the phase and amplitude of a coherent state. Similarly to classical signals, information can be demodulated through different flavors of coherent detection [3].

Traditionally, CV-QKD systems use a co-propagating laser signal that serves as *local oscillator* (LO) in the receiver [4]. This may open security loopholes as it allows the eavesdropper to manipulate the LO for individual qubits [5]. Furthermore, the channel losses have to be compensated for the co-propagating LO, requiring large optical power on the transmitter side. Later, more practical implementations using a pilot tone for synchronization and a separate local laser as LO were proposed [6]–[8].

For experimental CV-QKD setups it is common to define a loose and strict security assumption, where calibrated detector noise and loss is either attributed to the receiver or the eavesdropper [9]. Publications on experimental CV-QKD systems have worked under a loose security assumption so far.

Vulnerability to side channel attacks and possible counter measures [10] will not be covered by this paper.

II. Software defined CV-QKD

Here, a scheme is employed, where the transmitter and receiver operate with different laser frequencies. The detection is followed by an electrical or digital down-conversion in the classical domain, which is less sensitive to imperfections [11]–[13]. The employed signaling scheme can be seen in Fig. 1. From the point of view of the detector, only one component of the phase space is observed, the signal band and the mirror band cannot be distinguished. Because of the shift in frequency, both phase space components of the quantum signal can still be recovered but with a doubled noise bandwidth.

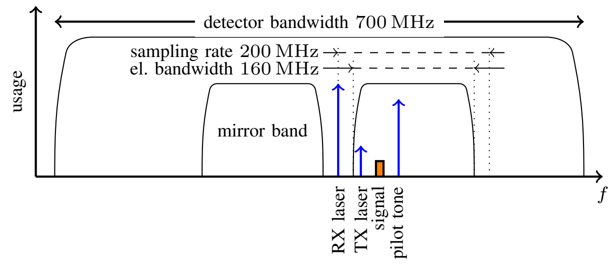

Fig. 1. Frequency allocation of quantum channel and pilot tone with respect to transmit and receiver laser frequency and receiver bandwidth.

The bandwidth of the quantum channel is only 10 MHz and the band with efficiency of this scheme is rather low. In return there are less sources of imperfections, which effectively reduces loss, noise, and the probability of side channel attacks in the optical domain. The achievable key rate and the supported reach with a strict security model benefit more from reducing the losses and noise in the system than from increasing the raw symbol rate (See Fig. 2). A detailed security analysis of this procedure will be given in a follow up paper.

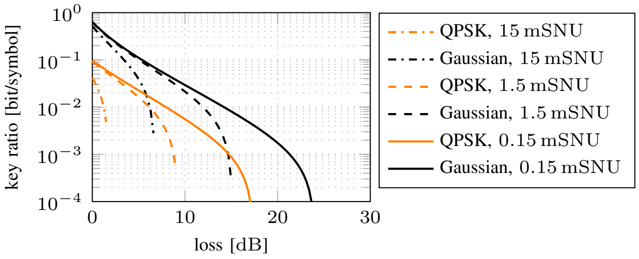

Fig. 2. Expected reach for different excess noise figures with Gaussian and QPSK modulation. The key rate is proportional to loss and bounded by noise.

A pilot tone is copropagated with the quantum signal to facilitate carrier frequency offset and phase noise compensation. The quantum signal is time interleaved with a training sequence for phase and clock recovery and frame synchronization. The quantum signal, training sequence, and pilot tone are generated and recovered in the digital domain, rendering this system as software-defined. The setup supports Gaussian and non-Gaussian modulation of the quantum signal, as far as it is supported by the DAC and ADC. This allows to use the protocols from [1], [2].

III. Loss and noise

A detailed analysis of the dominant sources of loss and noise will be given in the talk or poster following the block diagram in Fig. 3 similarly to [14].

The common figure of merit is the channel excess noise expressed in *shot noise units* (SNU), which is a normalization of the noise with respect to the shot noise measurement, i.e., the shot noise measurement itself has a variance of $1\,\mathrm{SNU}$. To simplify the notation *milliSNU* (mSNU) will be used throughout the paper $1000\,\mathrm{mSNU} = 1\,\mathrm{SNU}$. Please note that due to the phase diversity receiver structure, the excess noise measurement at the receiver has to be multiplied by two to express it in channel excess noise.

It is of high importance to make a difference between noise and loss. With a polarization diverse modulation and receiver structure the SNR at the receiver can be found as SNR $= \frac{T|\alpha_{\mathrm{TX}}|}{1+\xi}$, where T is the total transmittance, α_{TX} is the number of transmit photons per symbol, and ξ is the channel excess noise in SNU [13]. If the transmittance is reduced, the SNR is reduced by the same factor. The SNR can also be reduced by an increased excess noise. E.g., a $1\,\%$ reduction of the SNR could either be due to an approximately $0.04\,\mathrm{dB}$ higher loss or an excess noise increase by roughly $10\,\mathrm{mSNU}$. Although it makes no difference for the SNR, where the change comes from, there will be almost no change in key rate, if the change comes from an increased loss, while the key rate will drop dramatically, if the change comes from an increased noise (See Fig. 2).

IV. Pulse shaping and digitalization

The system at hand operates with a continuous-wave laser. The pulse shaping is performed in the digital domain followed by an electrical filter and possibly an optical filter at the transmitter and the reverse order at the receiver. The combination of digital, electrical and possibly optical filtering confines the quantum signal to its dedicated bandwidth with relaxed requirements for the analog filters. The out-of-band radiation is suppressed by at least $20\,\mathrm{dB}$. Due to the close to optimal matched filtering, almost all of the transmitted power can be detected by the receiver and the *signal-to-noise ratio* (SNR) is maximized. The measured SNR at the receiver, derived from a comparison of the transmitted and received signal, confirms this statement. The SNR estimate is almost identical with the theoretical SNR for given loss of the fiber and the optical components in the receiver.

For the rather low sampling rate of $200\,\mathrm{MSps}$ DACs and ADCs with a high resolution of $16\,\mathrm{bit}$ and $14\,\mathrm{bit}$, respectively, are available. With a dynamic range of approximately $86\,\mathrm{dB}$, the quantum signal can be combined with a pilot tone more than $30\,\mathrm{dB}$ stronger while only distortions smaller than $0.1\,\mathrm{mSNU}$ are introduced due to the quantization. The influence of imperfect quantization, like unequally distributed steps, can be neglected.

The conversion from digital to analog and back is not only a conversion between continuous and discretized values, but also between continuous and discretized time. The clock at the receiver can have a slightly different frequency and offset than the clock at the transmitter. Due to the high oversampling rate in the system, the error introduced by a timing offset is negligible. The DAC and ADC clocks drift by less than a few Hz, which can be corrected with high precision, by a sampling in the kHz range.

V. Transmitter imperfections

The signal is modulated before it is attenuated, which makes it possible to minimize all transmitter imperfections to negligible values. The electrical amplifier and the optical modulator are driven with low input power, which mitigates their non-linear behaviour. The inter-modulation products are suppressed by at least $30\,\mathrm{dB}$.

The quantum signal is shifted to an intermediate frequency and, therefore, the bias of the modulator cannot show up as noise. But, the bias of the modulator does show up as loss. The power meter captures approximately $99\,\%$ of the total transmit power. This includes the power in the pilot tone, the bias, and the quantum signal. As the power in the bias is unknown,

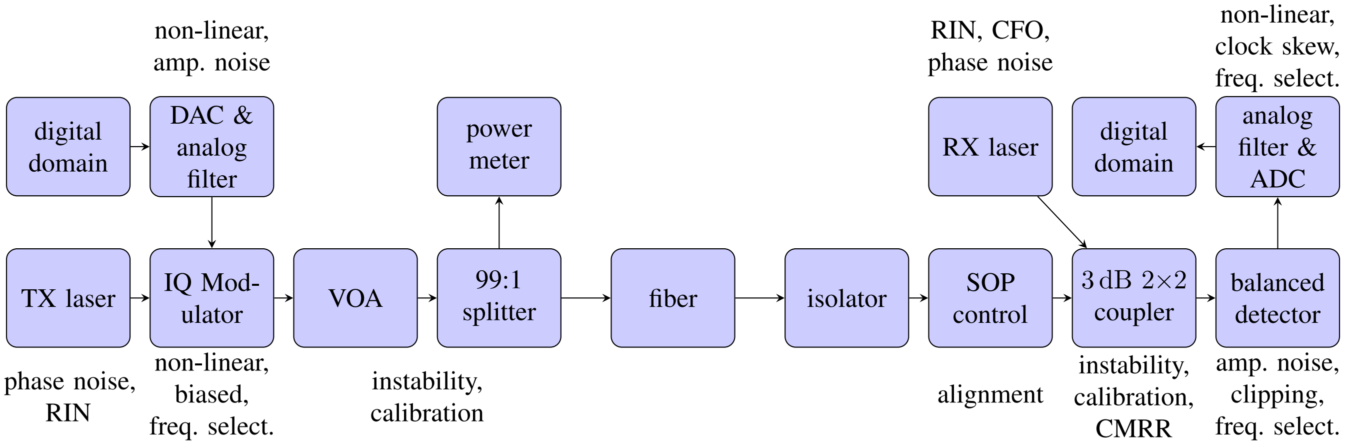

Fig. 3. Block diagram of transmitter and receiver including selected sources of loss and noise. Side channel protection is omitted to keep the plot simple.

the worst case assumption of no power in the bias has to be assumed, when the transmit power is estimated. The bias is typically $16\,\mathrm{dB}$ smaller than the total power, which means that only a small loss is connected to this effect.

The accuracy of the transmit power measurement has to be regarded as loss in the same fashion. The maximum power of a reasonable confidence interval has to be taken as worst case assumption. The total penalty of the transmit power measurement is in the order of a few percent, approximately $0.2\,\mathrm{dB}$. The exact transmit power has only a limited influence on the key rate.

VI. Receiver imperfections

The noise sources at the receiver are the limiting factors. Imperfect polarization alignment is purely loss in the described system. A reasonably good alignment reduces the connected loss below $0.2\,\mathrm{dB}$. *Carrier frequency offset* (CFO) is also purely loss. If the matched filter is shifted to an incorrect frequency the power in the quantum signal will not be captured. The CFO can be corrected almost perfectly introducing only negligible loss. But an imperfect phase noise suppression disturbs the quantum signal. The phase noise can come from the quantum channel and the pilot tone. With narrow linewidth lasers, a pilot tone quantum signal separation of $20\,\mathrm{MHz}$, and $30\,\mathrm{dB}$ more power in the pilot tone than in the quantum signal, more than $20\,\mathrm{dB}$ of phase noise can be compensated at an SNR of $-10\,\mathrm{dB}$. The remaining noise is in the order of $1\,\mathrm{mSNU}$ and can be mitigated even further.

The employed lasers are selected to have a very low *relative intensity noise* (RIN). The RIN measured at a single photo diode is $10\,\mathrm{mSNU}$. After a balanced detection, this noise is additionally suppressed by more than $30\,\mathrm{dB}$ of *common mode rejection ratio* (CMRR), which reduces this noise to a negligible value.

The most dominant sources of noise are the electronic noise of the detector and the accuracy of the noise measurement. The receiver side laser power is increased to a trade-off value. On the one hand, the ratio between the shot noise and the excess noise should be maximized, on the other hand the influence of saturation should be minimized. For high bandwidth systems the electronic noise is typically in the order of $250\,\mathrm{mSNU}$ and the system can only generate a key, if the noise is attributed to the receiver in a loose security assumption. Low bandwidth detectors with $10\,\mathrm{mSNU}$ electronic noise are commercially available. This noise variance still limits CV-QKD in general and the system at hand in particular to less than $20\,\mathrm{km}$ distance under a strict security assumption, where this noise is attributed to the eavesdropper. For communication systems an electronic noise $20\,\mathrm{dB}$ below the shot noise is already negligible. It is a challenging task, but there is no reason, why it should not be possible to reduce the noise and low noise detectors with down to $1\,\mathrm{mSNU}$ have been tailored [15].

The shot noise measurement $\hat{\sigma}^2_{\mathrm{sn}}$ of the system under investigation only varies with frequencies lower than $0.01\,\mathrm{Hz}$. These drifts are the temperature dependencies of involved components, dominated by the $3\,\mathrm{dB}$ coupler at the receiver. It is sufficient to do a noise calibration twice a minute to track these changes. The worst case value of a reasonable confidence interval has to be taken as the noise estimate $\hat{\sigma}^2_{\mathrm{sn}} - \Delta_{\sigma^2_{\mathrm{sn}}}$. With a bandwidth of $f_q = 10\,\mathrm{MHz}$, a measurement time t, and a $99\,\%$ confidence interval the accuracy can be found as $\Delta_{\sigma^2_{\mathrm{sn}}} \approx \frac{2.576\sqrt{2}}{\sqrt{f_q t}}$. The noise has to be averaged over roughly one second to get to an accuracy of $1\,\mathrm{mSNU}$ and one hundred seconds to get to an accuracy of $0.1\,\mathrm{mSNU}$. Additionally to the noise calibration, the excess noise has to be estimated from the conditional variance of the received signal in the parameter estimation step of the protocol, where random parts of the transmit signal are revealed for this purpose.

VII. Conclusion

A software-defined heterodyne CV-QKD architecture is presented. In the proposed scheme most of the complexity is shifted to the more flexible digital domain. This facilitates investigations, improves robustness and reproducibility, and gives accurate control over the noise in the system. The system is mainly limited by the electronic noise of the balanced detector and finite size effects. It can be expected that an improvement of the detector-noise characteristics will allow to work under strict security models over long distances.

References

[1] F. Grosshans and P. Grangier, “Continuous variable quantum cryptography using coherent states,” *Phys. Rev. Lett.*, vol. 88, p. 057902, Jan. 2002.

[2] A. Leverrier and P. Grangier, “Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation,” *Phys. Rev. A*, vol. 83, p. 042312, Apr. 2011.

[3] K. Kikuchi, “Fundamental of coherent optical fiber communications,” *J. Lightwave Technol.*, vol. 34, no. 1, pp. 157-179, Aug. 2015.

[4] P. Jouguet et al., “Experimental demonstration of long-distance continuous-variable quantum key distribution,” *nature photonics*, vol. 7, pp. 378-381, Apr. 2013.

[5] E. Diamanti et al., “Practical challenges in quantum key distribution,” *npj Quantum Inform.*, vol. 2, p. 16025, Nov. 2016.

[6] B. Qi et al., “Generating the local oscillator locally in continuous-variable quantum key distribution based on coherent detection,” *Phys. Rev. X*, vol. 5, p. 041009, Oct. 2015.

[7] D. Huang et al., “High-speed continuous-variable quantum key distribution without sending a local Oscillator,” *Optics Lett.*, vol. 40, no. 16, pp. 3695-3698, Aug. 2015.

[8] D. Soh et al., “Self-referenced continuous-variable quantum key distribution protocol,” *Phys. Rev. X*, vol. 5, p. 041010, Oct. 2015.

[9] F. Grosshans et al., “Quantum key distribution using gaussian-modulated coherent states,” *Nature*, vol. 421, pp. 238-241, Jan. 2003

[10] E. Diamanti and A. Leverrier, “Distributing secret keys with quantum continuous variables: principle, security and implementations,” *Entropy*, vol. 17, no. 9, pp. 6072-6092, Aug. 2015.

[11] S. Kleis and C. G. Schaeffer, “Heterodyne coherent scheme for long distance quantum key distribution using a real local oscillator,” in *42nd Europ. Conf. Optical Commun.*, Dsseldorf, Germany, 2016.

[12] Z. Qu, I. B. Djordjevic and M. A. Neifeld, “RF-subcarrier-assisted four-state continuousvariable QKD based on coherent detection,” *Optics Lett.*, vol. 41, pp. 5507-5510, Dec. 2016.

[13] H. H. Brunner et al., “A low-complexity heterodyne CV-QKD architecture,” in *19th Int. Conf. Transparent Optical Networks*, Jul. 2017.

[14] F. Laudenbach et al., “Continuous-variable quantum key distribution with gaussian modulation the theory of practical implementations,” *arXiv*:1703.09278, Mar. 2017.

[15] D. Huang, P. Huang, D. Lin and G. Zeng, “Long-distance continuous-variable quantum key distribution by controlling excess noise,”, *nature Scientific Reports*, vol. 6, p. 19201, Jan. 2016.