Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator

Fabian Laudenbach[1,2,*], Bernhard Schrenk[2], Christoph Pacher[2], Michael Hentschel[2], Chi-Hang Fred Fung[3], Fotini Karinou[3], Andreas Poppe[3], Momtchil Peev[3], and Hannes Hübel[2]

[1]Security & Communication Technologies, Center for Digital Safety & Security,
AIT Austrian Institute of Technology GmbH, Donau-City-Strasse 1, 1220 Vienna, Austria
[2]Quantum Optics, Quantum Nanophysics & Quantum Information, Faculty of Physics,
University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria
[3]Optical and Quantum Laboratory, Munich Research Center,
Huawei Technologies Duesseldorf GmbH, Riesstrasse 25-C3, 80992 Munich, Germany

[*]mail: fabian.laudenbach@ait.ac.at

We present a pilot-assisted coherent intradyne reception methodology for CV-QKD with true local oscillator. An optically phase-locked reference tone, prepared using carrier-suppressed optical single-sideband modulation, is multiplexed in polarisation and frequency to the 250 Mbaud quantum signal in order to provide optical frequency- and phase matching between quantum signal and local oscillator. Our concept allows for high symbol rates and can be operated at an extremely low excess-noise level, as validated by experimental measurements.

1 Introduction

Quantum key distribution using continuous variable (CV-QKD) [1–5] is currently regarded as one of the main contenders for a full-scale deployment of quantum cryptography. Its advantages over traditional qubit-based implementations include higher key rates and, more importantly, the ability to use established telecom technology (I/Q-modulation, Mach-Zehnder pulse carving, coherent detection) rather than complex and costly components required for discrete-variable QKD (single-photon sources and -detectors). Unlike counting polarisation- or phase-encoded single photons, in CV-QKD the raw key is established by encoding the quadrature components of weak coherent states $|\alpha\rangle = |I_A + iQ_A\rangle$. The information read-out is performed by coherent detection where the weak quantum signal is mixed with an optically strong reference laser, the so-called local oscillator (LO), at a balanced beamsplitter. The difference in optical power at the output ports of the beamsplitter is then proportional to the quadrature I or Q, depending on the phase Θ of the LO: $\Delta P \propto |\alpha_{\mathrm{LO}}| \, (I \cos\Theta + Q \sin\Theta)$. The PIN diodes used for the power measurement can operate at high rates (up to $\sim 10\,\mathrm{GHz}$) and are at the same time highly efficient and low-priced. This compares beneficially to avalanche photo diodes used in discrete-variable QKD which are both limited in the detection rate (by their dead time after a counting event) and quantum efficiency but are at the same time several times as expensive. Moreover, the facilitated integration of balanced detectors onto photonic chips crucially supports the miniaturisation of CV-QKD receivers for ubiquitous quantum-information applications.

The coherent-detection scheme requires for the signal laser and the LO to retain a stable and well-known frequency- and phase relation. One natural and simple way to provide for this requirement is to have the signal and the LO originate from the same laser source, as it was implemented in early realisations of CV-QKD [6–9]. This (often called ‘self-homodyning’ or ’in-line local oscillator’) approach, however, requires for the LO to be jointly transmitted with the quantum signal which not only severely limits the total LO power available at the receiver (due to channel loss), but also disturbs the quantum- (and other DWDM) channels in the fibre. More importantly even, it opens grave security loopholes due to possible side-channel attacks that an eavesdropper can perform on the LO [10–15].

In order to provide for security of the key-exchange procedure and compatibility with telecom fibre infrastructure, it is therefore unavoidable to generate the LO locally at the receiver (‘*true* local oscillator’, or sometimes ‘*local* local oscillator’, LLO). Since in this scheme the signal and LO laser are mutually independent, the LLO scheme requires a phase- (and frequency) synchronisation to allow for coherent detection. As already widely established in classical communication, carrier-phase recovery does not necessarily require to adjust and lock the relative phase and frequency between the two lasers *ahead* of measurement. Instead, the measurement can be performed with an arbitrary relative phase, yielding a corresponding rotation of Bob’s phase-space coordinates with respect to Alice’s. If Bob has knowledge about the phase- and frequency difference between the two lasers, he can counter-rotate his coordinate axes *post-measurement* and reconcile his data with Alice's reference frame. In standard quadrature-amplitude modulation (QAM) used for telecommunication, the phase- and frequency correction is directly extracted from the data signal. Since in CV-QKD the quantum signal itself is too weak to allow for a precise phase- and frequency measurement, Alice will prepare a strong second signal, represented by a fixed and well-known point in phase space. Originating from the same laser as the quantum states, this reference signal carries all the frequency and phase information that Bob needs in order to estimate the phase- and frequency difference between his laser and Alice's. He will mix his local oscillator with the quantum and reference signal and measure the quadratures of both independently. The measurement of the reference signal allows him to monitor the phase drift over time and to apply the reverse rotation to the individual quantum measurements accordingly.

In recent demonstrations of the above method a time-multiplexed scheme was adopted, where strong reference pulses were temporally interleaved with the quantum signal [16–18]. Although straightforward to implement, this method comes with certain impairments. Firstly, in the time-multiplexing scheme the additional synchronization pulses will reduce the rate of the quantum signal since Alice needs to reserve periodic time slots in her pulse train for the reference signal. Secondly, the quadratures of the quantum signal are not measured at exactly the same time as the synchronisation quadratures, i.e. phase changes which are fast compared to the symbol rate will not be compensated. Finally, if the quantum- and the reference signal are measured with the same balanced receivers, the allowed optical power of the reference pulse is restricted by the saturation limit of the PIN diodes (which is usually very low for low-noise receivers as required for CV-QKD). On the other hand, routing of signal- and reference pulses to designated receivers respectively (low-noise for quantum, high-saturation limit for pilot) requires cumbersome and fast switching, when the two are multiplexed in the time degree of freedom only.

In addition to the sequential transmission of signal- and reference pulses, Ref. [19] proposes a scheme based on modulation displacement, where each symbol encoded by Alice is added to a fixed and well-known offset in amplitude $|\Delta|$ and phase θ_Δ. Therefore the transmitted coherent states are represented as $|\alpha\rangle = |I_A|\Delta|\cos\theta_\Delta + Q_A|\Delta|\sin\theta_\Delta\rangle \equiv |\alpha_A + \Delta\rangle$ where α_A is a weak coherent state carrying the quantum information and the offset Δ is a stronger coherent state carrying the phase reference. Bob performs simultaneous measurements on the states in the I- and Q-basis (in CV-QKD literature often referred to as 'heterodyne' measurement) and extracts the phase estimation from the displacement of Alice's modulation. Unlike the methods based on time-multiplexing, in this approach the accuracy of the phase estimation is not independent from the modulation variance (since a higher amplitude of the quantum signal will, paradoxically, reduce the SNR of the offset-phase measurement). Moreover, this scheme suffers from the trade-off that the balanced receivers have to operate at low electronic noise (required for CV-QKD security) but at the same time need to have a sufficiently high saturation limit in order to allow for an accurate measurement of the strong offset state.

Starting in 2016, we've been demonstrating that multiplexing of the quantum signal and a pilot tone in the polarisation- and frequency domain [20–22] is a promising alternative to sequential modulation of reference pulses. In 2017, a second group demonstrated the advantages of frequency multiplexing [23], however without exploiting the polarisation degree of freedom and without optical suppression of the pilot carrier. In their setup, the frequency-upconverted quantum signal and pilot tone were of the same polarisation and detected using one and the same balanced heterodyne receiver. (Note the different meaning of the term 'heterodyne' in the terminology of telecommunications (data out of baseband) and CV-QKD (simultaneous measurement of both bases). In this article we adhere to the telecom jargon.)

In this work we present a complete pilot-assisted coherent *intradyne* reception methodology (frequency offset between transmitter laser and LO much smaller than the symbol rate, baseband detection of quantum data) in which an optically phase-locked reference tone is multiplexed to the actual quantum signal in both, modulation frequency *and* polarisation. The quantum signal is generated using quadrature-phaseshift-keying (QPSK) at a symbol rate of $R_{\text{sym}} = 250\,\text{Mbaud}$; the pilot tone was generated using carrier-suppressed optical single-sideband modulation at $f_P = 1\,\text{GHz}$. As opposed to Ref. [23], the exploitation of the polarisation degree of freedom allows us to (1) efficiently avoid crosstalk of the strong pilot to the weak quantum signal, (2) perform adequate power-levelling of signal and pilot as well as (3) the use of optimised receivers, accounting for the particular requirements of the weak quantum signal and strong pilot tone, respectively. Moreover, our intradyne-reception architecture can be operated at a much lower sampling rate compared to schemes based heterodyne detection.

2 Pilot-Tone Assisted Continuous-Variables Detection Scheme with Local Oscillator at Receiver

The experimental transmitter setup is illustrated in Fig. 1. The optical carrier at $\lambda_T = 1550.12\,\text{nm}$ with a linewidth of 400 kHz (*Teraxion PS-LM*) was amplitude-modulated from continuous wave to 250 MHz pulses using a Mach-Zehnder pulse carver (*Optilab IML-1550-40-PM*) and, subsequently, fed into a polarisation-multiplexing ('PolMux') IQ modulator (*Fujitsu FTM1977HQA*). The PolMux allows for independent modulation of the orthogonally polarised pilot tone and quantum signal, preserving their locked frequency and phase relation. Modulation of the quantum tributary yielded a QPSK signal at a symbol rate of $R_{\mathrm{sym}} = 250\,\mathrm{Mbaud}$. The pilot tone was modulated with a $f_P = 1\,\mathrm{GHz}$ cosine function, representing a fixed symbol, static in phase space. The quantum- and pilot modulators were controlled by an arbitrary-waveform generator (AWG, *Keysight M9502A*). For preparation of the pilot we performed single-sideband modulation with suppressed optical carrier (oCS-SSB). Figure 2(a) illustrates the frequency spectrum of the pilot tone after SSB with and without carrier suppression. In order to ensure security of the protocol, the quantum signal is supposed to be sufficiently weak (depending on the channel length and noise level: $\langle n\rangle \sim 0.1$–$10$). On the other hand, the pilot tone is required to be as strong as possible to allow for an accurate phase measurement. Therefore, we performed a polarisation-dependent attenuation, reducing the optical power of the quantum signal by $-23\,\mathrm{dB}$ with respect to the pilot tone. This power levelling between pilot and data signal was performed while preserving optical phase locking and facilitated through selective attenuation on the polarisation tributaries using a polarisation controller and a fibre-based polarization beamsplitter. Using a monitor in the reflected path (ρ in Fig. 2(b)), the optical pilot power at 1 GHz is suppressed in order to maximise the pilot (π) and, at the same time, attenuate the quantum signal (τ) at the output port. The inset in Fig. 2(b) shows the eye diagram of the QPSK quantum signal with the characteristic dips.

The receiver setup is illustrated in Fig. 3. An optically free-running local oscillator (LO, *Teraxion PS-NLL*) with a narrow linewidth of $\Delta f < 100\,\mathrm{kHz}$ and a power of 12 dBm was used for coherent optical detection. Manual frequency alignment between f_T and f_{LO} was performed by current- and temperature-tuning in order to ensure an optical-frequency deviation much smaller than the symbol rate of the quantum data $|f_T - f_{\mathrm{LO}}| < R_{\mathrm{sym}}$. Coherent intradyne reception of both tributaries was performed by use of a polarisation-diversity 90° hybrid (*Kylia COH28-X*) which mixed the quantum signal and pilot tone with the local oscillator and routed them to their designated balanced detectors. Two pairs of balanced detectors (one for each quadrature component of quantum signal and pilot) were used for opto-electronic signal conversion, each pair tailored to the specific needs of the respective signal tributary: The quantum data was detected using low-noise receivers with a bandwidth of 360 MHz, a clearance of 20 dB (Fig. 3(b)) and a common-mode rejection ratio (CMRR) of $\sim 40\,\mathrm{dB}$ (Fig. 3(c)), allowing for low excess noise and therefore a higher secure-key rate. A set of high-bandwidth ($> 1\,\mathrm{GHz}$) PIN/TIA receivers (Fig. 3(c)) was chosen for the stronger and therefore more robust pilot tone which requires a larger bandwidth and optical saturation limit but can, in return, tolerate more noise than measurements of the quantum signal since the pilot itself is not security-sensitive to eavesdropping attacks. Subsequently, the electrical I/Q signals were post-amplified, acquired in blocks of 2^{20} samples (≈ 1.05 megasamples) by a real-time oscilloscope (*Agilent Technologies DSO-X 91604A*) and fed to offline digital signal processing (DSP).

The individual DSP steps are illustrated in Fig. 4. The first step consists of signal conditioning by means of spectral filtering of noise in the excess base- and pass-bandwidth. The frequency offset between LO (f_{LO}) and transmitter emission wavelength (f_T) was estimated by comparison of detected and nominal pilot frequency and subsequently corrected. Next, a carrier-phase recovery was performed. For this purpose the optical phase drift between the transmitted signal and the LO was quantified by the rotation of the received pilot tone in phase space. Since the quantum signal was optically phase-locked to the pilot and had therefore experienced the same phase changes, the measured I/Q quadratures could be corrected using the rotation of the pilot tone which had been robustly acquired at high signal-to-noise ratio. Finally, a CV-QKD parameter estimation was performed on the recovered quantum QPSK data to determine the excess noise and, therefore, the quality of the pilot scheme.

3 Continuous-Variable Key-Transmission Performance

The experiment was conducted over four different channel lengths using standard single-mode fibres of total length 1 km, 4 km, 13 km and 40 km, respectively. The first three channels were simulated by fibre spools in the lab, the latter one was provided by a 40 km deployed fibre in the city of Vienna.

Figure 5(a) illustrates the observed phase drifts, with peak-drift rates of up to $6.9\,\mathrm{rads}/\mu\mathrm{s}$, that were corrected post-measurement. A phase-space illustration of the results before and after digital signal processing is found in Fig. 5(b).

In order to evaluate the performance of our pilot-tone concept, we performed the calibration of our measurements as well as the parameter estimation along the lines of Ref. [5]. As primary indicator of the experimental quality we investigated the excess noise ξ, i.e. the quadrature variance in addition to the obligatory quantum shot noise. We define the excess noise referring to the *receiver's* input port (as opposed to the transmitter), such that the total quadrature variance at Bob is represented as

$$V_B(\hat{I}) = V_B(\hat{Q}) = TV_{\mathrm{mod}} + N_0 + \xi, \tag{1}$$

where T is the total channel transmittance, V_{mod} is the modulation variance as applied by Alice (equal to twice the mean photon number per symbol) and N_0 is the quantum shot noise ($N_0 = 1$ in shot-noise units, SNU). (Note that in our notation the total excess noise comprises the electronic noise of the detectors, in literature often labelled as ν_{el}.) Since we performed simultaneous measurement of I and Q, we split the incoming signal into two arms, one for each quadrature basis. The variance in each arm is therefore

$$V'_B(\hat{I}) = V'_B(\hat{Q}) = \frac{T}{2}V_{\mathrm{mod}} + N_0 + \frac{\xi}{2}, \tag{2}$$

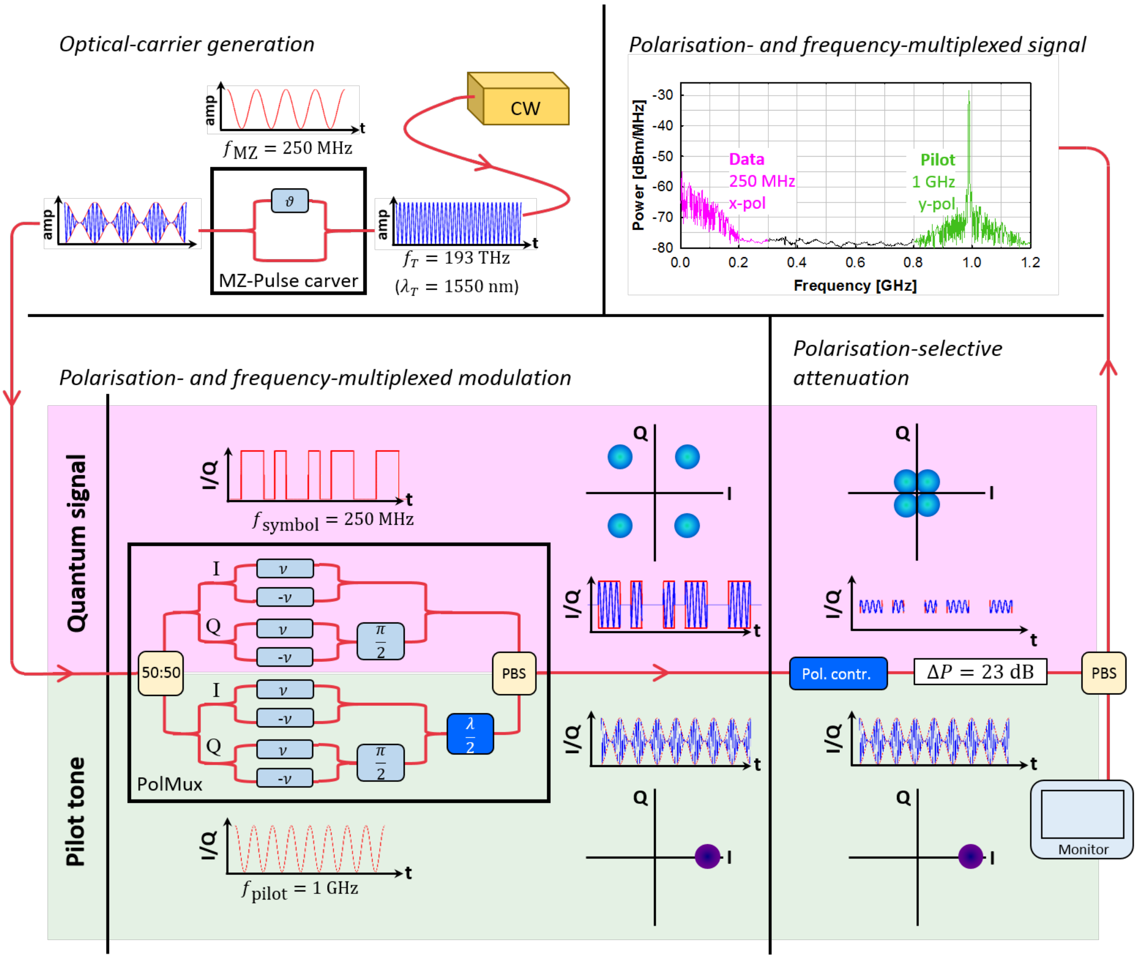
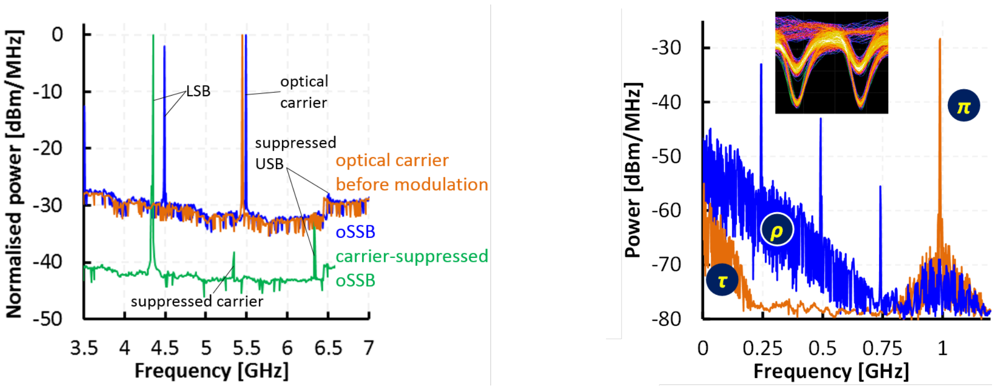


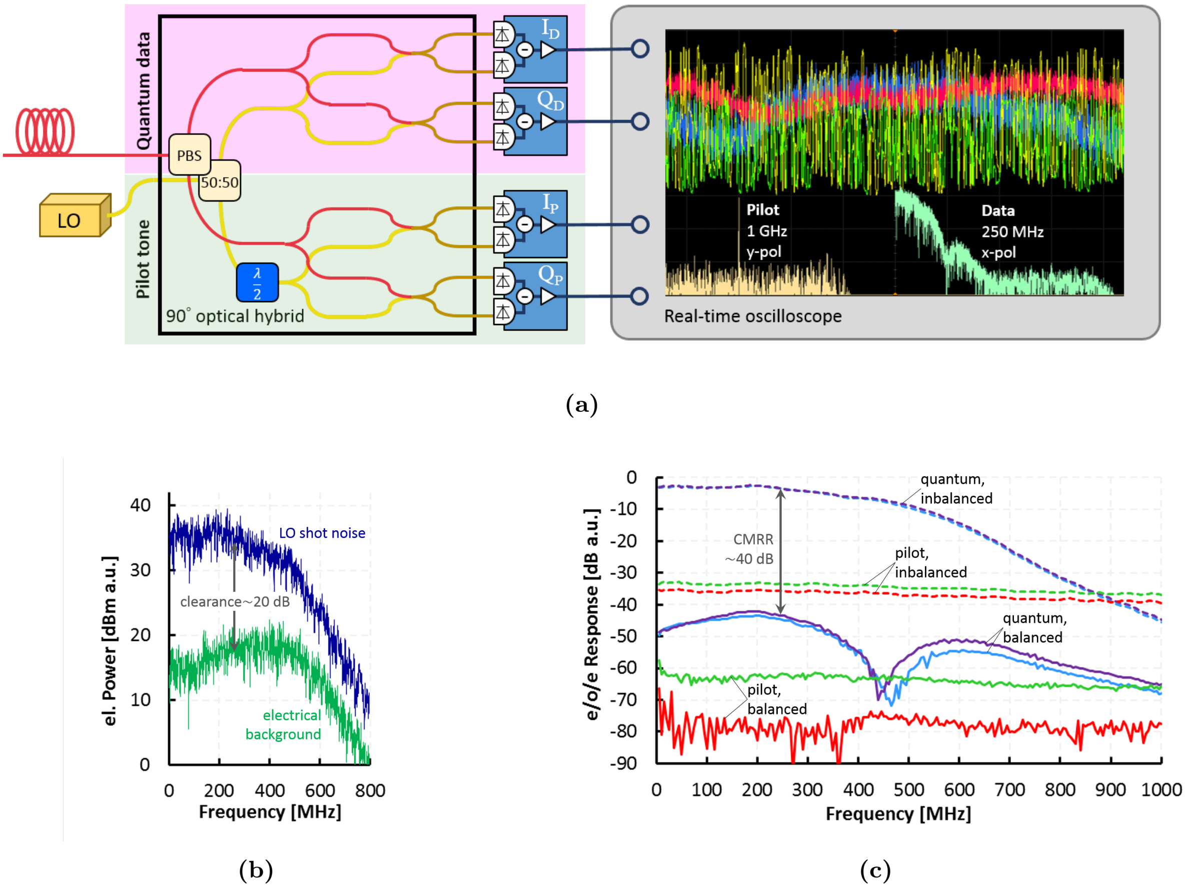
Figure 1: Schematics of the transmitter setup. A 250 MHz pulse train, carved by Mach-Zehnder amplitude modulation of a 1550 nm CW laser, is fed into the polarisation-multiplexed I/Q modulator (PolMux). The PolMux branches the pulses into two halves where the quantum signal and pilot tone are I/Q modulated independently (light-blue boxes representing phase rotations and the dark-blue box representing a polarisation rotation by a 90° half-wave plate). The quantum branch is modulated with a 250 Mbaud QPSK pattern, driven by a pseudorandom binary sequence of length $2^7 - 1$ (PRBS7). For the pilot tone, we performed optical single-sideband modulation with suppressed carrier, driven by a 1 GHz cosine function (see Fig. 2(a)). After recombination of the two branches under orthogonal polarisation, the quantum signal was attenuated (see Fig. 2(b)) to adhere to the security requirements of CV-QKD while at the same time retaining a strong pilot amplitude to allow for a high SNR, as required for accurate phase recovery.



(a)

(b)

Figure 2: (a) Optical single-sideband pilot tone (mixed to an intermediate frequency of 5.5 GHz) without (blue) and with (green) optical carrier suppresion. (b) Signal spectra after polarisation-selective attenuation. Using an in-line fibre polariser, we suppressed the pilot tone at the monitored output port of a polarising beamsplitter (ρ). Consequently, the transmitted output was fed with a strong pilot (π) and weak quantum signal (τ), the power difference amounting to ~ 23 dB.



(a)

(b)

(c)

Figure 3: (a) Schematics of the receiver setup. An optical 90°-polarisation-diversity hybrid separates the incoming compound signal with respect to polarisation and mixes the quantum signal and pilot tone with the LO and routes them to the respective balanced receivers (one receiver for each basis in the quantum- and pilot branch). On the right side a screenshot of the oscilloscope traces illustrates the measurement data obtained by the four receivers: The QPSK quantum data with respect to time is depicted by the yellow (I) and green (Q) line, the periodic pilot tone by the smoother blue and red line. The bottom of the oscilloscope illustrates the pilot and quantum data in the frequency domain. (b) Shot-noise response and intrinsic electronic noise of the quantum receivers. The clearance is defined as the ratio of the two and indicates the receiver noise ξ_{det} in shot-noise units. (c) CMRR of quantum- and pilot receivers. The lines correspond to the I- and Q detectors of the quantum signal (purple and blue) and the pilot tone (green and red), respectively. At balanced response (solid lines), both PIN diodes of one detector were fed with the same optical power; to measure the imbalanced response (dashed lines), one of the two diodes was disconnected from the optical signal.

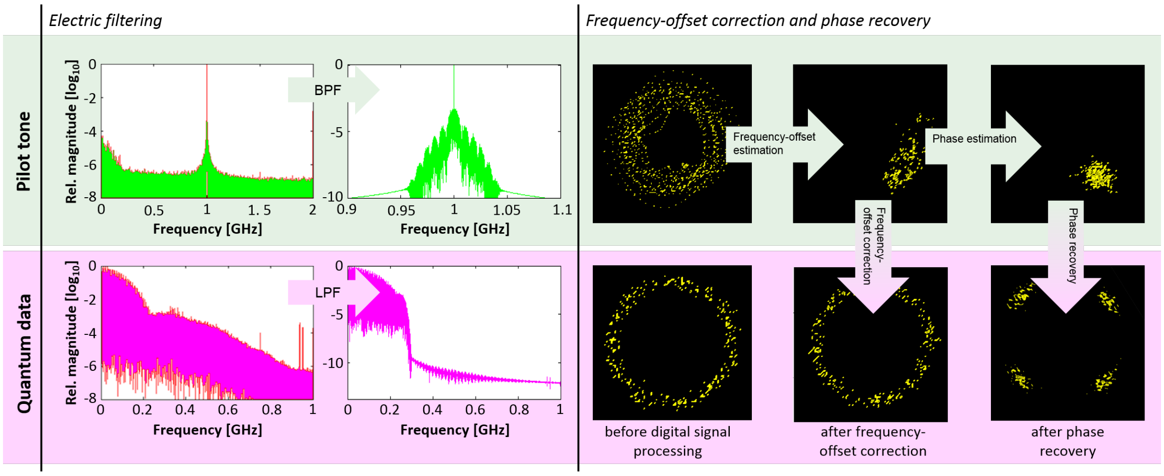


Figure 4: Sequence of the digital signal processing (DSP). The pilot tone is bandpass-filtered (BPF) with a FWHM of 4 MHz, the quantum data is lowpass-filtered (LPF) with 250 MHz cutoff. The phase-space constellations for the acquired pilot and the quantum data are shown before and after DSP. The optical-frequency offset $|f_T - f_{\text{LO}}|$ as well as the phase drift between LO and transmitter laser turns the 1-point pilot constellation and the QPSK constellation of the quantum signal into a ring. However, the optical phase of the pilot can be sampled by virtue of its high signal-to-noise ratio. In this way, the relative phase drift is estimated and applied to compensate the frequency offset and the phase drift of the quantum data. The original QPSK data can be recovered with good quality, as evidenced by the distinguishable constellation points.

where we doubled the electronic detection noise of each basis ($\xi_{\text{det}} = 2\xi'_{\text{det}}$) before integration into the total excess noise ξ such that Eq. (2) holds. In contrast to the total variance above, the conditional variance $V_{B|A}$ relates Bob's measurement results to the symbols modulated by Alice (and therefore requires for Alice or Bob to disclose a certain fraction of their data). In general, it is represented as (here in the I-basis)

$$V'_{B|A}(\hat{I}) = V\left(\frac{T}{2}\hat{I}_A - \hat{I}_B\right). \tag{3}$$

In a discrete-modulation alphabet (like QPSK) $V'_{B|A}$ is simply the variance of all measurements that have been associated to one and the same symbol during the bit disclosure. Since the conditional variance in each basis is $V'_{B|A} = N_0 + \xi/2 \overset{\text{SNU}}{=} 1 + \xi/2$, the excess noise could be computed using

$$\xi = 2 \cdot (V'_{B|A} - 1). \tag{4}$$

As another key parameter, the signal-to-noise ratio (SNR), was determined using

$$\text{SNR} = \frac{\frac{T}{2}V_{\text{mod}}}{1 + \frac{\xi}{2}} = \frac{V'_B}{V'_{B|A}} - 1. \tag{5}$$

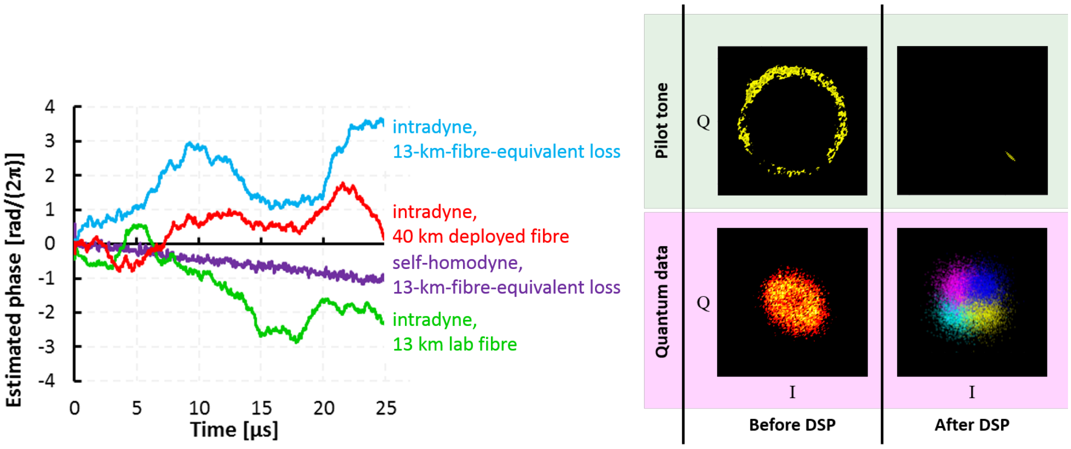
Table 1 summarises the numeric experimental results over four distances using optical carrier-suppressed single sideband modulation (oCS-SSB) of the pilot, processing 2^{20} samples ($\approx$ 1.05 megasamples) for each measurement. In order to find the proper conversion of our measurements from voltages to shot-noise units, we performed a sample of calibration measurements (eight shot-noise measurements and four measurements of the electronic noise). Table 1 lists the noise results for the case where the conversion was performed using the averaged calibration measurements as well as the results that we obtained when we, pessimistically, only used the one calibration measurement that yielded the highest conditional variance, and hence the largest excess noise ξ. Moreover, for both calibration approaches, we list the total measured excess noise as well as the excess noise *excluding* the intrinsic detection noise of the balanced receivers ξ_{det}. This is relevant for the relaxed assumption that the receivers in Bob's lab are regarded as trusted devices and therefore do not contribute to Eve's information. As indicated by the table, the total measured excess noise ξ_{tot} for the respective transmission distances amounted to values between 0.022 SNU and 0.036 SNU for averaged calibration and 0.053 SNU and 0.067 SNU for worst-case calibration. As for the excess noise excluding the detection noise $\xi_{\text{tot}} - \xi_{\text{det}}$, we obtained values between 0.0010 SNU and 0.015 SNU (averaged calibration), or respectively, between 0.030 SNU and 0.044 SNU (worst-case calibration). The two bottom lines of the table depict our results using oSSB without suppressed carrier. Comparison of the results indicates an obvious advantage of optical carrier suppression yielding excess-noise figures which are lower by factors of 2–3, as illustrated in Fig. 6. This noise disparity indicates the limitations of oSSB without suppressed carrier where a non-zero frequency offset Δf between the receiver (LO) and the strong optical carrier of the pilot causes a detrimental beat note in the low-frequency regime. Note that the numeric excess-noise results listed in Table 1 refer to input port of the receiver R, i.e. $\xi := \xi_{RX} = T\xi_{TX} = 2\xi'$, where RX and TX denote receiver and transmitter, and ξ' is the measured excess noise in one of the two bases, I and Q.

For the sake of comparison, a self-homodyne reception scheme has been evaluated as well. For this purpose the optical carrier of the transmitter was reused as LO for coherent optical detection at the receiver side rather than using an independent, local LO. Comparing the self-homodyning results with the ones obtained using our pilot-assisted intradyne-detection scheme with suppressed optical carrier, we observed no penalty whatsoever in terms of excess noise.

Our results indicate that the novel method of polarisation- and frequency multiplexing allows for higher symbol rates and, at the same time, lower excess noise compared to the currently more established time-multiplexing schemes [16–18]. The method was demonstrated for QPSK modulation of the quantum signal but can, however, be implemented just as well for any modulation alphabet, including continuous Gaussian modulation for which the security analysis is understood best. The estimated final secure-key rate depends on several additional parameters which are beyond scope of this local-LO demonstration: the reconciliation efficiency β, the frame-error rate FER, the fraction of the raw key ν that has to be disclosed during parameter estimation, the effects of finite blocklengths, and finally, the actual modulation alphabet that is used in the respective implementation of the scheme. To give an example, assuming $\beta = 0.97$, FER $= 0.05$, $\nu = 0.25$, Gaussian modulation, coherent attacks, relaxed security assumptions (detection noise not attributed to Eve) and averaged calibration, our experimental parameters obtained for the 40 km deployed fibre ($R_{\text{sym}} = 250$ Mbaud, $V_{\text{mod}} = 12.5$, SNR $= 0.62$, $\xi_{\text{tot}} = 0.026$, $\xi_{\text{tot}} - \xi_{\text{det}} = 0.0047$) correspond to an asymptotic secure-key rate of 3.0 Mbits/s over 40 km.

4 Conclusion

We reported a novel reception method for CV-QKD with a free-running true local oscillator. We used a pilot tone of strong optical amplitude, multiplexed in frequency and polarisation to the quantum data, to establish the necessary phase reference. Experimental evaluation with a symbol rate of 250 Mbaud and over a transmission distance of up to 40 km yielded a low excess noise, confirming the robustness of the method. Not only closes our scheme the security loophole opened by a transmitted LO – the novel approach of polarisation- and frequency multiplexing furthermore allows for higher symbol rates compared to time-multiplexing methods and for the deployment of optimised detectors for the quantum signal (low noise)



(a) (b)

Figure 5: (a) Accumulated phase drifts at four different measurement scenarios. The light-blue and purple line represent transmission over a short fibre where a channel loss corresponding to 13 km has been simulated using a variable attenuator. (b) Phase-space representation of pilot- and quantum data before and after digital-signal processing, i.e. frequency-offset correction and phase recovery.

					averaged calib.		*worst-case calib.*	
Channel length [km]	$\boldsymbol{T}$	$\boldsymbol{V_{\text{mod}}}$	$\boldsymbol{\langle n_B \rangle}$	**SNR**	ξ_{tot}	$\xi_{\text{tot}} - \xi_{\text{det}}$	ξ_{tot}	$\xi_{\text{tot}} - \xi_{\text{det}}$
1	0.60	3.0	0.92	0.90	0.036	0.015	0.067	0.044
4	0.53	4.1	1.1	1.06	0.023	0.0016	0.054	0.031
13	0.35	3.7	0.65	0.64	0.022	0.0010	0.053	0.030
40	0.10	12.5	0.63	0.62	0.026	0.0047	0.057	0.034
6 (no supp. carr.)	0.50	6.4	1.5	1.44	0.079	0.057	0.11	0.090
13 (no supp. carr.)	0.35	8.5	1.5	1.41	0.087	0.066	0.12	0.098

Table 1: Measurement results after raw-key transmission over four channel lengths. The amount of excess noise that is attributed to the eavesdropper depends not only on whether one operates under the trusted-detector assumption ($\xi_{\text{Eve}} = \xi_{\text{tot}} - \xi_{\text{det}}$), but also on the way the calibration is performed: For the averaged calibration we used the mean of all the calibration measurements, for the worst-case calibration we only used the most disadvantageous one. The noise results indicate a strong advantage of optical carrier suppression over SSB without suppressed carrier (two bottom lines). Note that all excess-noise figures describe the quadrature variance in addition to the shot noise at the *receiver* side and that the measured excess noise in each basis is $\xi/2$.

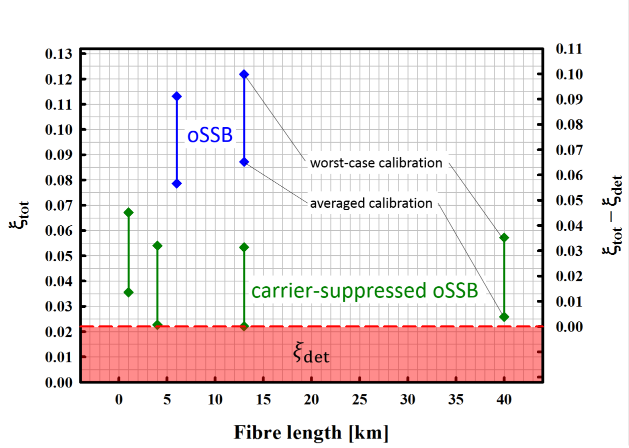


Figure 6: Illustration of the measured excess noise at optical single-sideband modulation with suppressed optical carrier (green) and oSSB without carrier suppression (blue). The lower diamonds describe the noise results after averaged calibration, the upper ones represent the noise of the same measurement, but under worst-case calibration. The red area on the bottom represents the measured detection noise which can, under relaxed security assumptions, be regarded as trusted noise. In this case the noise attributed to an eavesdropper is $\xi_{\text{tot}} - \xi_{\text{det}}$ (right axis).

and pilot (high bandwidth and saturation limit), respectively. Moreover, the cross-polarised preparation of signal and pilot tone as well as the suppression of the optical pilot carrier proved to be efficient methods to avoid crosstalk from the strong reference signal to the quantum channel. The raw-key transfer could be performed at a low-noise level, introducing no noise penalty with respect to inherently phase-stabilised self-homodyning. Due to the demonstrated advantages, we believe that the proposed pilot-tone scheme is a promising candidate for any future implementation of high-performance CV-QKD transceivers.

Acknowledgements

We acknowledge support from G. Humer, R. Lieger and E. Querasser for fruitful discussions and valuable technical support.

References

[1] F. Grosshans and P. Grangier, *Continuous variable quantum cryptography using coherent states*, Phys. Rev. Letters **88**, 057902 (2002).

[2] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, *Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables*, arXiv:quant-ph/0306141 (2003).

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution*, Rev. Mod. Physics **81**, 1301 (2009).

[4] C. Weedbrook, S. Pirandola, and T. C. Ralph, *Continuous-variable quantum key distribution using thermal states*, Phys. Rev. A **86**, 022318 (2012).

[5] F. Laudenbach, C. Pacher, C. H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, *Continuous-Variable Quantum Key Distribution with Gaussian Modulation – The Theory of Practical Implementations*, arXiv:1703.09278 (2017).

[6] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, *Experimental demonstration of long-distance continuous-variable QKD*, Nature Phot. **7**, 378 (2013).

[7] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, *Field test of a continuous-variable quantum key distribution prototype*, New J. Phys. **11**, 045023 (2009).

[8] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, *Quantum key distribution over 25 km with an all-fiber continuous-variable system*, Phys. Rev. A **76**, 042305 (2007).

[9] B. Qi, L. L. Huang, L. Qian, and H. K. Lo, *Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers*, Phys. Rev. A **76**, 052323 (2007).

[10] H. Häseler, Tobias Moroder, and Norbert Lütkenhaus, *Testing quantum devices: Practical entanglement verification in bipartite optical systems*, Phys. Rev. A **77**, 032303 (2008).

[11] J. Z. Huang, C. Weedbrook, Z. Q. Yin, S. Wang, H. W. Li, W. Chen, G. C. Guo, and Z. F. Han, *Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack*, Phys. Rev. A **87**, 062329 (2013).

[12] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, *Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol*, Phys. Rev. A **87**, 052309 (2013).

[13] H. Qin, R. Kumar, and R. Alléaume, *Saturation attack on continuous-variable quantum key distribution system*, Proc. SPIE **8899**, 88990N (2013).

[14] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, *Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution*, Phys. Rev. A **87**, 062313 (2013).

[15] 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*, Phys. Rev. A **88**, 022339 (2013).

[16] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, *High-speed continuous-variable QKD without sending a local oscillator*, Opt. Lett. **40**, 3695 (2015).

[17] 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*, Phys. Rev. X **5**, 041009 (2015).

[18] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R.M. Camacho, J. Urayama, and M. Sarovar, *Self-referenced continuous-variable quantum key distribution protocol*, Phys. Rev. X **5**, 041010 (2015).

[19] A. Marie and R. Alléaume, *Self-coherent phase reference sharing for continuous-variable quantum key distribution*, Phys. Rev. A **95**, 012316 (2017).

[20] B. Schrenk and Hannes Hübel, *Pilot-Assisted Local Oscillator Synchronisation for CV-QKD*, in Proc. of QCrypt 2016, Washington DC, USA, 195 (2016).

[21] B. Schrenk, F. Laudenbach, F. Fung, C. Pacher, A. Poppe, R. Lieger, D. Hillerkuss, E. Querasser, G. Humer, M. Hentschel, M. Peev, and H. Hübel, *High-rate continuous-variable quantum key distribution with pilot-disciplined local oscillator*, in Proc. of European Conference on Optical Communication (ECOC 2017), Gothenburg, SWE, P2.SC6.q10 (2017).

[22] F. Laudenbach, B. Schrenk, C. Pacher, R. Lieger, E. Querasser, G. Humer, M. Hentschel, C. H. F. Fung, A. Poppe, M. Peev, and H. Hübel *Pilot-Disciplined CV-QKD with True Local Oscillator*, in Proc. of QCrypt 2017, Cambridge, UK, Mo33 (2017).

[23] S. Kleis, M. Rueckmann, and C. G. Schaeffer, *Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals*, Opt. Lett. **42**, 1588 (2017).