Pilot-Disciplined CV-QKD with True Local Oscillator

F. Laudenbach, B. Schrenk, C. Pacher, R. Lieger, E. Querasser, G. Humer, M. Hentschel, H. Hübel
AIT Austrian Institute of Technology, Center for Digital Safety & Security, Donau-City-Str. 1, 1220 Vienna, Austria.
Author e-mail address: fabian.laudenbach@ait.ac.at

C.H.F. Fung, A. Poppe, M. Peev
Huawei Technologies Duesseldorf GmbH, Optical and Quantum Laboratory, GRC, ERI, 80992 Munich, Germany.

Abstract: We present a pilot-assisted coherent intradyne reception methodology for CV-QKD with true local oscillator. An optically phase-locked reference tone 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. Experimental measurements validate the concept and indicate the potential for Mb/s key rates for link lengths in the 10 km range.

1. Introduction

Continuous variable QKD (CV-QKD) is currently thought of to be one of the main contenders for a full-scale deployment of QKD. Its main advantage is the ability to use established photodiode technology and higher background suppression due to extremely narrowband electronic (digital) filters, but with the drawback of the need for coherent detection. In the early realisations of CV-QKD [1] the strong local oscillator (LO) was jointly transmitted with the quantum signal. Due to power restrictions and side-channel attacks [2] it is unavoidable to generate the LO locally at the receiver. Such a scheme will still need synchronisation between the transmitter laser and the now true local LO (LLO), since the quantum signal is too weak to yield direct phase information. Experimental demonstrations were recently carried out using LLO designs [3–5]. In these works, a time-multiplexed scheme was adopted, where strong reference pulses were sent interleaved with the quantum signal. The reference pulses were coherently detected using the LLO, and hence any phase drift could be monitored and used for correction of the quantum data.

In this work we present a new LLO scheme based on pilot-assisted coherent intradyne reception methodology in which an optically phase-locked reference tone is multiplexed in both, frequency and polarization, to the actual quantum signal. The advantages over a time-multiplexed approach are: Firstly, the symbol rate of the quantum signal is not reduced by synchronisation pulses, and secondly, the quadratures of the quantum signal are exactly measured at the same time as the synchronization tone. As will be demonstrated the pilot-tone scheme allows for exact phase/frequency estimation simultaneously to the quantum signal and does not compromise signal bandwidth. Additionally, saturation that can easily occur with strong synchronisation pulses is avoided in case of the pilot-assisted scheme.

2. Pilot-Tone Assisted Continuous-Variables Detection Scheme with Local Light Source at Receiver

The experimental setup of the CV-QKD system is illustrated in Fig. 1. At Alice's transmitter the optical carrier at λ_T = 1550.12 nm (linewidth 400 kHz) is modulated in inphase/quadrature (I/Q) phase space in both polarization tributaries by either data (representing the quantum states) at a symbol rate of R_Q = 250 Mbaud and a tone at f_P = 1 GHz. This yields a QPSK quantum signal and a pilot tone that is multiplexed in both, frequency and polarization, while it is optically phase locked to the data in virtue of the photonic-integrated PolMux-IQ modulator. Optical single-sideband modulation is chosen for the pilot tone in order to suppress mirror frequencies resulting in detrimental beat noise in case of coherent homodyne (λ_R=λ_T) and intradyne ($\lambda_R \approx \lambda_T$) detection. While the data signal is strongly attenuated (A_T) to ensure transmit power levels (P_{TX}) of 4.2 photons per data symbol, the pilot tone is preserved at a relative level of +23 dB in order to yield a good signal-to-noise ratio after reception through Bob. This power levelling between pilot and data preserves optical phase locking when it is facilitated through selective attenuation on the polarization tributaries using a fibre-based polarization beamsplitter (PBS_T). The compound signal is then transmitted over a channel comprising a 12.8 km long ITU-T G652.B-compatible standard single-mode fibre (SMF).

At Bob an optically unlocked LO (linewidth <10 kHz) and a power of 12 dBm was used for coherent optical detection. Alignment of optical emission frequencies ν_T and ν_R was made by current/temperature tuning in order to ensure $\delta\nu = |\nu_R - \nu_T| << R_Q$. Coherent intradyne reception is then conducted in both tributaries through a polarisation-diversity 90° hybrid. Since this hybrid performs a quantum-heterodyne measurement for each polarization instead of a simple homodyne measurement, the optical output consists of the I_X and Q_X variable in case of the quantum data. Two pairs of balanced detectors have been used for opto-electronic signal conversion, each of them tailored to the specific needs of the respective signal tributary. The quantum data (I_X,Q_X) is detected using low-noise receivers with a common-mode rejection ratio (CMRR) of ~40 dB in order to ensure lowest excess noise and lowest reduction in secure key rate. The CMRR is retained at such a high value by periodic probing of the detector balance using a RF probe tone at f_R directly emitted by Alice (ε) and received by Bob with deactivated LO. In case of optimal balancing, the RF probe tone is cancelled out. A set of high-bandwidth PIN/TIA receivers have been chosen for the stronger and therefore more robust pilot tone (I_Y,Q_Y), which requires a larger bandwidth but can yet accommodate more noise. The received signal spectra for the quantum and pilot tributary are shown in Fig. 1 as insets Q and P.

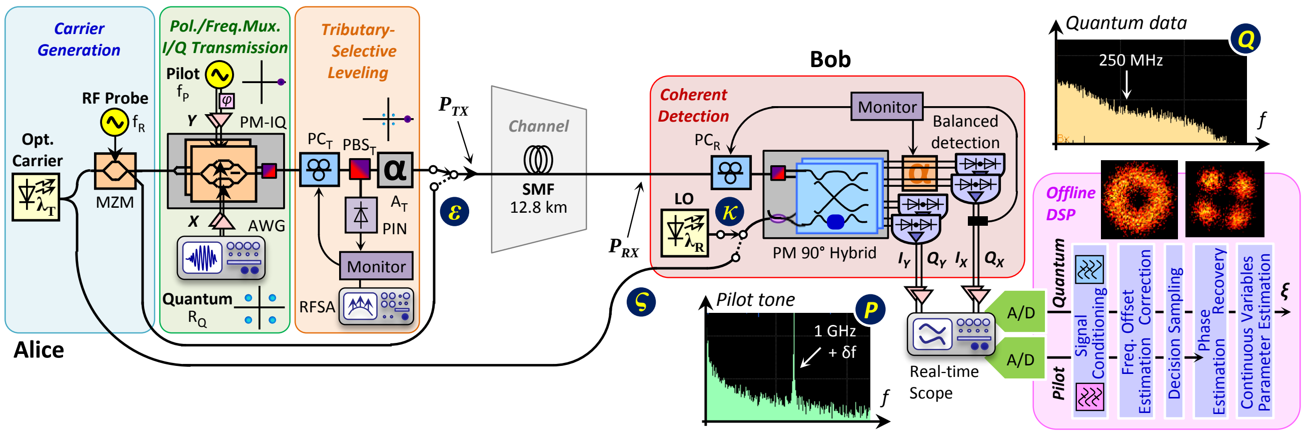

Fig. 1. Pilot-disciplined continuous-variables transmission systems with true local oscillator at the receiver.

The electrical I/Q signals are then post-amplified, acquired by a real-time oscilloscope and fed to off-line digital signal processing (DSP). The DSP first performs signal conditioning by filtering noise in the excess bandwidths. The frequency offset δν is then estimated through comparison of detected and nominal pilot frequency and corrected. Next, a carrier-phase recovery is performed: The optical phase drift between transmitted optical carrier and the LO is quantified by the rotation of the received pilot in phase space. Since the quantum signal is optically phase-locked to the pilot and has therefore experienced the same phase drift, the measured I/Q quadratures can be corrected using the rotation of the pilot, which has been acquired at high signal-to-noise ratio. Finally a parameter estimation according to [6] is performed on the recovered quantum QPSK data to obtain a measure on the channel transmission T and the excess noise ξ and therefore on the Holevo information which is an upper bound of the mutual information between Eve and Bob.

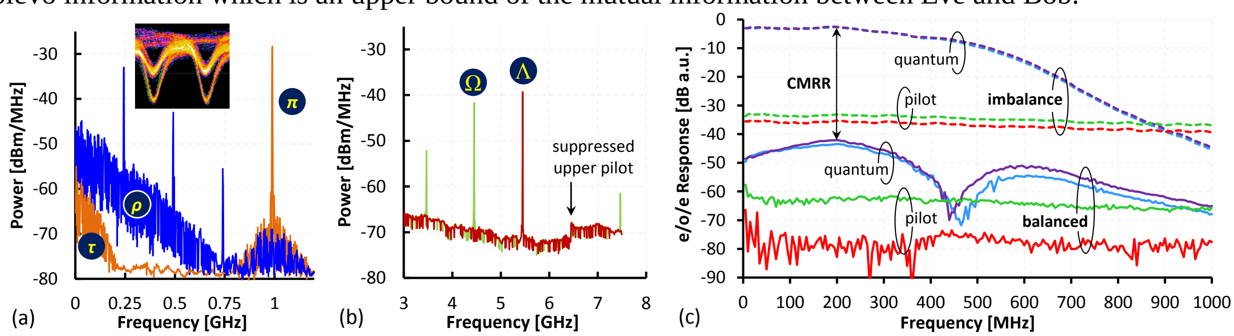

Fig. 2. (a) Signal spectra after tributary-selective attenuation at both ports of the power leveller. (b) Optical single-sideband pilot tone after heterodyning with the LO. (c) CMRR of balanced quantum and pilot receivers.

3. Characterisation of Sub-Systems and Signal Evolution

The transmitted signal spectra are presented in Fig. 2(a) at both output ports of the polarisation-selective attenuator (PBS_T). The signal that is reflected (ρ) towards the monitor path aims to suppress the pilot tone at 1 GHz. This corresponds to a maximised pilot (π) at the transmitted port towards the channel, which goes along with a highly attenuated quantum signal (τ). The ratio among integrated power of π and τ corresponds to the polarisation extinction ratio of PBS_T. The inset in Fig. 2(a) shows the eye diagram of the QPSK quantum signal as superposition of patterns occurring for the actual quantum data stream. The characteristic dips when switching between the four I/Q phase states and a constant power during the data symbol can be observed.

The transmitted optical single-sideband pilot is shown in Fig. 2(b) after heterodyning with the LO, shifting the optical carrier (Λ) to an intermediate frequency of 5.4 GHz. When modulating at the pilot tone frequency (Ω) the tone in the upper sideband is suppressed. As such the pilot signal enables an accurate estimation of the experienced optical phase shift after fibre transmission and coherent reception.

The response of several balanced detectors is presented in Fig. 2(c). A high CMRR of 39.5 and 40.8 dB is obtained at 200 MHz for the quantum receivers, for which an opto-electronic bandwidth of 360 MHz can be inferred. This indicates that saturation is avoided even in case of a strong LO while excess noise can be effectively suppressed. In case of the pilot receivers the bandwidth exceeds 1 GHz, however, at lower CMRR.

4. Continuous-Variables Transmission Performance and Discussion of Results

The I/Q constellations for the acquired pilot and the quantum datas are shown in Fig. 3(a) before and after DSP. The optical phase drift between LO and transmitter laser turns the 1-point pilot constellation (A) and the QPSK constellation of the quantum signal (C) into a torus. However, the optical phase of the pilot can be measured in virtue of its high signal-to-noise ratio. In this way a drift as shown in Fig. 3(c) is estimated and applied to compensate the phase of the quantum data. Peak drift rates of 6.9 rads/µs have been experienced and require active compensation. The original QPSK can be resembled with good quality, as it is evidenced by the distinguishable constellation points (D). The excess noise, directly measured by comparison of the conditional variance with the quantum shot noise, amounted to $\xi = 0.0358$ SNU for each basis (referring to the receiver side). Together with our modulation variance of $V_{mod} = 8.34$ SNU this allows for a **transmission over 12.8 km with 2.87 Mbit/s asymptotic secure-key rate** (assuming a reconciliation efficiency of $\beta = 0.97$).

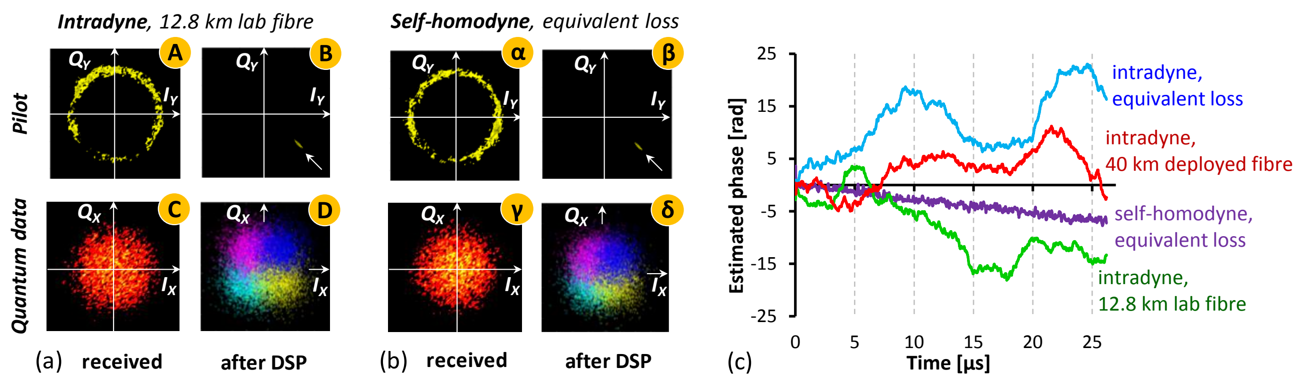

Fig. 3. Received and corrected constellations after DSP for (a) intradyne reception with locking of transmit and LO laser, (b) self-homodyne reception using the transmit laser also as LO. (c) Estimated optical phase of the pilot.

For purposes of comparison the 12.8 km fibre was replaced with a 6.3 km fibre yielding an excess noise of $\xi = 0.0316$ SNU per basis which corresponds to a **secure-key rate of 34.2 Mbit/s** (with $V_{mod} = 6.3$ SNU and $\beta = 0.97$). Finally, a self-homodyne reception scheme has been evaluated as well. For this purpose the optical carrier of the transmitter (λ_T) is being reused for coherent optical detection at Bob (ς) rather than using the LO (κ). In this way the penalty of the LO synchronisation scheme can be evaluated. We experienced a much lower phase drift of 0.25 rads/µs and measured an excess-noise parameter of $\xi = 0.0379$ SNU for each basis. We therefore conclude that no implementation penalty is introduced by the LLO scheme.

5. Conclusions and Outlook

A novel reception method for CV-QKD has been presented. The LO at the receiver was continuously locked by a pilot tone multiplexed in frequency and polarisation to the quantum data. Experimental measurements over 12.8 (6.3) km of transmission fibre confirm the robustness of the scheme through a secure-key rate of 2.9 (34.2) Mb/s. The implementation penalty in comparison with self-homodyne detection has been found to be negligible, which renders the proposed pilot tone scheme as a promising candidate for CV-QKD transceivers. Refinements of the setup (further noise suppression and longer transmission distances) as well as the creation of secure key with our QKD-post-processing software are scheduled for summer 2017.

6. References

[1] P. Jouguet et al., "Experimental demonstration of long-distance continuous-variable QKD", Nature Phot. **7**, 378 (2013).

[2] H. Häseler et al., "Testing quantum devices: Practical entanglement verification in bipartite optical systems", Phy. Rev. A. **77**, 032303 (2008).

[3] B. Qi et al., "Generating the local oscillator locally in continuous-variable quantum key distribution based on coherent detection", Phys. Rev. X. **5**, 041009 (2015).

[4] D. Soh et al., "Self-referenced continuous-variable quantum key distribution protocol", Phys. Rev. X. **5**, 041010 (2015).

[5] D. Huang et al., "High-speed continuous-variable QKD without sending a local oscillator", Opt. Lett. **40**, 3695 (2015).

[6] F. Laudenbach et al., "Continuous-Variable Quantum Key Distribution with Gaussian Modulation – The Theory of Practical Implementations", arXiv:1703.09278 (2017).