Pilot-Free Digital Clock Synchronization for Continuous-Variable Quantum Key Distribution

Patrick Matalla, Md Salek Mahmud, Christian Koos, and Sebastian Randel

Institute of Photonics & Quantum Electronics (IPQ), Karlsruhe Institute of Technology (KIT), Germany.
patrick.matalla@kit.edu, sebastian.randel@kit.edu

Abstract *A feedforward blind digital clock synchronization method is investigated for continuous-variable quantum-key distribution. We demonstrate timing synchronization for an 1-GBd QPSK signal over a 20 km quantum channel at signal-to-noise ratios as low as -20 dB and various clock frequency offsets.*

Introduction

Fundamentally secure communication networks are essential for protecting our economy and society from cyber threats. During the past years a number of quantum key distribution (QKD) systems have been successfully demonstrated and first commercial products are deployed by government agencies and authorities. In the longer term, a quantum communication infrastructure could enable additional functionalities alongside QKD, such as digital signatures, authentication, and secret sharing schemes like e-voting[1]. QKD was first demonstrated with single photons and information is encoded, e.g., into the their polarization or phase and the secret key is established upon detection of individual photons. This so-called discrete-variable (DV) QKD requires, however, dedicated hardware components such as single-photon detectors. Recently, an alternative approach, referred to as continuous-variable (CV) QKD has attracted significant attention in the research community, since it allows to reuse components like inphase/quadrature modulators (IQMs) and balanced photodetectors (BPDs) originally developed for the telecommunications market[2].

In contrast to classical telecommunication links, CV-QKD links are operated in the vacuum noise limit at signal-to-noise ratios (SNR) of -10 dB or below, with a noise bandwidth matching the symbol rate. This makes it necessary to revisit the digital signal processing (DSP) algorithms for coherent optical receivers. In systems adding the local oscillator at the receiver, the carrier frequency and phase recovery as well as the polarization de-rotation can be solved by adding pilot tones or symbols[3]. Moreover, the symbol clock frequency and phase needs to be recovered at the receiver side, which can be achieved by adding additional pilots[4].

In this paper, we demonstrate through numerical simulations and by evaluating measured waveforms that it is possible to recover the symbol timing from a 1-GBd quadrature-phase shift keying (QPSK) signal detected with a heterodyne coherent receiver even at the vacuum noise limit while the receiver clock offset is as large as 10 parts per million (ppm). We obtain this in an optimized feedforward timing recovery structure with a timing estimator based on the Barton and Al-Jalili algorithm[5].

Pilot-Free Digital Timing Synchronization

A time delay τ of a received signal $x(t)$ corresponds to a linear phase shift $\exp(\mathrm{j}\,2\pi f\tau)$ in the frequency-domain. The algorithm investigated in this work exploits the spectral redundancy of a QPSK signal with root-raised cosine spectral shape with roll-off factor ρ in order to estimate the timing phase. To do so, the N-point FFT $\{X_n\}$ of the sampled receive signal is computed. Afterwards, a clock tone is generated by calculating the cross-correlation of the upper sideband (USB) and lower sideband (LSB). The phase of the clock tone is now proportional to the clock phase offset. Accordingly, the timing estimation $\hat{\tau}$ is obtained as

$$\hat{\tau} = \frac{1}{2\pi} \arg \left\{ \sum_{n=(1-\rho)N/4}^{(1+\rho)N/4-1} X_n X^*_{n+\frac{N}{2}} \right\} .$$

Due to the cross-correlation of the LSB and USB, random noise is effectively suppressed while the clock tone is preserved. This effect is particularly useful in systems with extremely low SNR, such as in CV-QKD. To investigate the performance of the synchronization for low SNR, a simulation of the entire feedforward clock recovery architecture was implemented. Besides the timing estimation according to Eq. 1, this also includes the buffer-

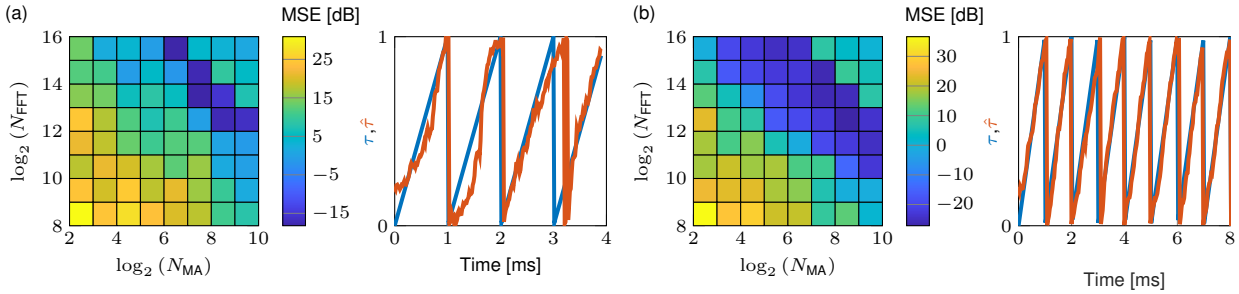

Fig. 1: Simulated MSE of the timing estimation for a FFT size N and averaging length N_{MA} parameter sweep and actual and estimated timing phase for (a) SNR=-20 dB, ρ=1, and a clock offset of 0.5 ppm as well as (b) SNR=-15 dB, ρ=0.7, and a clock offset of 1 ppm.

ing of the signal and the interpolation. Fig. 2 shows the complete processing chain used for the balanced heterodyne detection in this work. For

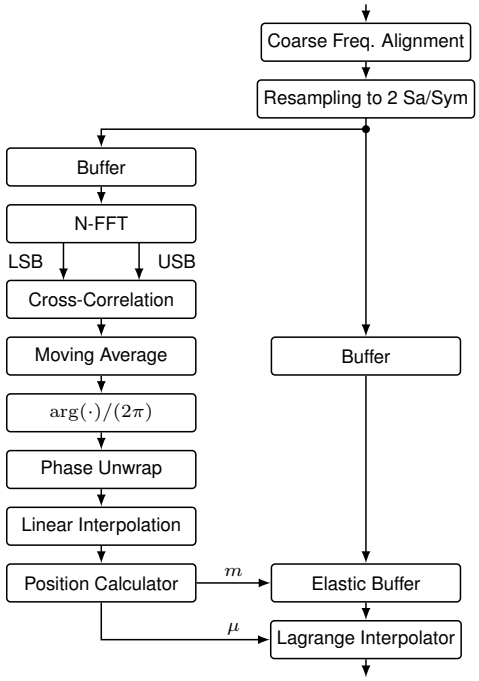

Fig. 2: DSP chain with feedforward clock synchronization.

the feedforward architecture, the signal is split into two paths. The first is used to estimate the clock phase, while in the second the signal is buffered for the duration of the estimation and then delayed by an integer multiple m of the sampling period in an elastic buffer and additionally by a fractional sampling period μ by a 5-th order Lagrange interpolator. The timing estimator path starts with a buffer as well. This allows an overlapping of the N-sample-long blocks, such that the temporal resolution of the time estimation is increased. In this work, an overlap of 50% was applied. Next, the timing estimation algorithm is applied. The oversampling ratio of the signal must be chosen such that no aliasing occurs. An oversampling of two was chosen in this work. In addition to optimizing the FFT-size, the cross-correlation is smoothed by a moving average filter of length N_{MA} in the complex plane to make the timing estimation less susceptible to noise. Finally, the timing phase is unwrapped over several unit intervals and linearly interpolated according to the resolution of the signal sequence. Finally, a position calculator determines the integer and fractional delay as mentioned earlier. More detailed explanations of the hardware implementation on field programmable gate arrays (FPGAs) and comparisons between different feedforward architectures are provided in[6],[7]. For the simulation, a random QPSK symbol sequence was generated, which is oversampled twice and pulse shaped to a root-raised cosine (RRC) spectrum. After adding white Gaussian noise, a constant sampling frequency offset is applied followed by a matched receive filter. The performance metric is the mean squared error (MSE) of the timing estimate $\hat{\tau}$ from the set timing offset τ calculated in decibels.

Figure 1 (a) shows the simulation results for an SNR of -20 dB. For such a case, effective noise suppression is mandatory. To ensure that the clock tone extends over several frequency bins over which the cross-correlation is formed, a high roll-off factor of ρ=1 was chosen. The FFT-size as well as the moving average filter length determine the noise reduction, but limit the synchronization bandwidth[7]. It can be seen that the timing synchronization becomes increasingly better with larger FFT-size and averaging. If the averaging is too large, the synchronization can no longer follow the clock frequency offset and the performance decreases accordingly. Fig. 1 (a), right, shows the best performance for N=8192 and N_{MA}=128 and demonstrates how the timing estimate follows the actual timing phase. Fig. 1 (b) shows a scenario with a roll-off of 0.7, as it was used in the experiment. A higher SNR of -15 dB was simulated with a higher clock frequency offset of 1 ppm. The higher SNR allows the use of smaller FFT blocks and less averaging. At

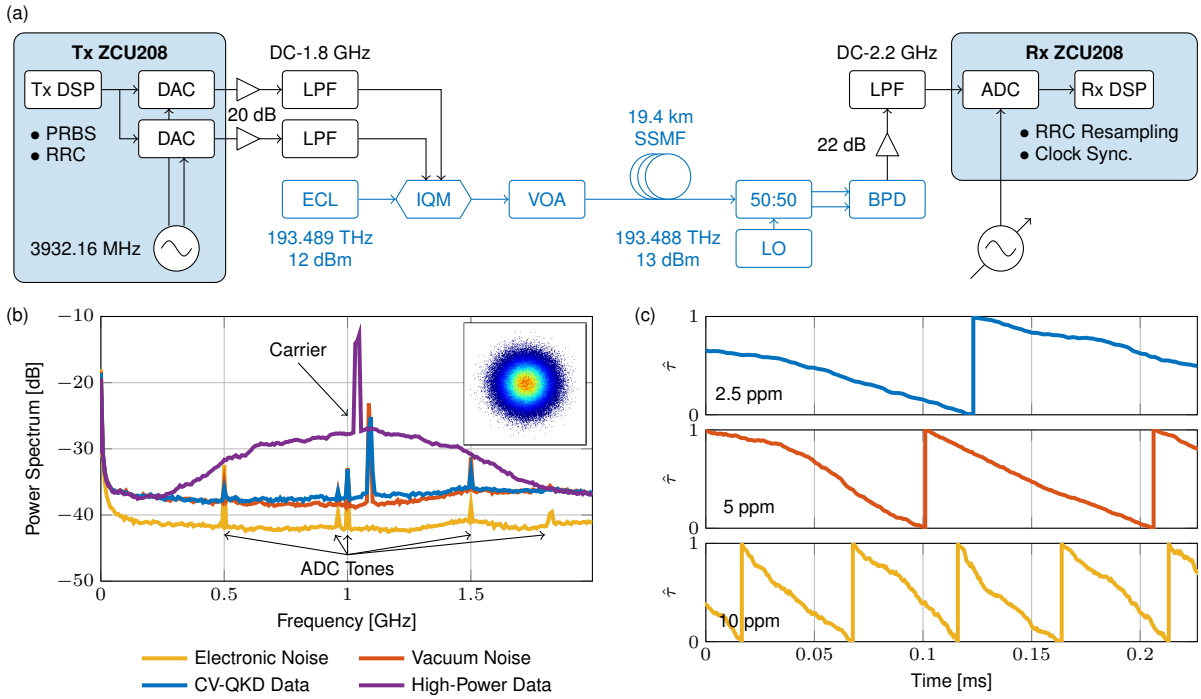

Fig. 3: (a) Experimental setup. (b) Various spectra obtained for the CV-QKD system over an around 20 km long quantum channel. (c) Timing estimates following various clock frequency offsets.

the same time this results in a synchronization at higher clock frequency offsets and it can successfully follow an offset of 1 ppm using N=4096 and N_{MA}=256. Regarding the implementation complexity, the moving average filter is simply an accumulating FIFO and thus can be implemented without significant resources. The latency caused by the large FFT blocks and the averaging can be easily adjusted by the buffer in feedforward architectures, a feature which would not easily be possible in a feedback architecture.

Experimental Validation

Figure 3 (a) shows the experimental setup to validate the timing synchronization. A PRBS15 sequence is generated in real-time at 2 Gbit/s, mapped to QPSK symbols and pulse-shaped in the transmitter-side Xilinx ZCU208 RF-System-on-Chip (RF-SoC) running at a sampling clock of 3932.16 MHz. The signal is amplified and the spectral images are supressed by a lowpass filter (LPF) before they are fed into an IQM, which modulates the optical carrier generated by an external cavity laser (ECL) at a frequency of 193.489 THz with optical power of 12 dBm. The optical signal is then attenuated using a variable optical attenuator (VOA) and transmitted over 19.4 km of standard single-mode fiber (SSMF). At the receiver-side, a free-running local oscillator (LO) at 193.488 THz with 13 dBm optical power is mixed with the signal for heterodyne coherent reception in a BPD. To optimally drive the ADC of a receiver-side RF-SoC, an RF amplifier with 22 dB gain is used. The ADC is driven by an external synthesizer to set a defined clock frequency offset of either 10 kHz, 20 kHz or 40 kHz. After the ADC, the sampled signal is written into a block-RAM and read out for offline processing following the DSP chain shown in Fig. 2. Figure 3 (b) reveals that the CV-QKD signal operates close to the vacuum noise level. As shown in (c), it is possible to detect and follow different clock frequency offsets despite the low SNR. For 10 ppm clock frequency offset, N=1024, and 64-fold averaging and for 5 and 2.5 ppm the same parameters were used.

Conclusions

We have presented a pilot-free digital feedforward clock synchronization scheme based on the timing estimation algorithm of Barton and Al-Jalili in simulation and in experiment, for application in CV-QKD. In this context, we have shown that operation near the vaccum noise level is possible even at clock-frequency offsets as high as 10 ppm. This paves the way towards simplified CV-QKD systems, which can operate without auxiliary signals and pilot tones and use matured optical transceivers and DSP hardware from the telecommunications market.

References

[1] European Commission. “Shaping europe’s digital future”. (2023), [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (visited on 05/05/2023).

[2] F. Laudenbach, C.Pacher, C. F. Fung, *et al.*, “Continuous-variable quantum key distribution with gaussian modulation - the theory of practical implementations”, *Advanced Quantum Technologies*, vol. 1, no. 1, p. 1 800 011, 2018. DOI: 10.1002/qute.201800011.

[3] T. A. Eriksson, R. S. Luís, K. Gümüs, *et al.*, “Digital self-coherent continuous variable quantum key distribution system”, in *2020 Optical Fiber Communications Conference and Exhibition (OFC)*, 2020, 1–3, paper T3D.5.

[4] H.-M. Chin, N. Jain, U. L. Andersen, D. Zibar, and T. Gehring, “Digital synchronization for continuous-variable quantum key distribution”, *Quantum Science and Technology*, vol. 7, no. 4, p. 045 006, Jul. 2022. DOI: 10.1088/2058-9565/ac7ba2. [Online]. Available: https://dx.doi.org/10.1088/2058-9565/ac7ba2.

[5] S. Barton and Y. Al-Jalili, “A symbol timing recovery scheme based on spectral redundancy”, in *IEE Colloquium on Advanced Modulation and Coding Techniques for Satellite Communications*, 1992, pp. 3/1–3/6.

[6] P. Matalla, M. S. Mahmud, C. Fuellner, C. Koos, W. Freude, and S. Randel, “Hardware comparison of feedforward clock recovery algorithms for optical communications”, in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, San Francisco, CA, USA, 2021, pp. 1–3, paper Th1A.10.

[7] P. Matalla, M. S. Mahmud, C. Fuellner, W. Freude, C. Koos, and S. Randel, “Real-time feedforward clock recovery for optical burst-mode transmission”, in *2022 Optical Fiber Communications Conference and Exhibition (OFC)*, San Diego, CA, USA, 2022, pp. 1–3, paper M2H.2.